Deny Any/Any 규칙이 뒤따르는 경우 DNS 허용 규칙이 일치하지 않음

목차

- 문제
- 환경
- 해결
- 원인
- 관련 콘텐츠

문제

인터넷 액세스 정책이 DNS 트래픽을 허용하기 위해 Permit Any/Any 규칙을 구성한 다음 정책 하단에서 Deny Any/Any 규칙을 사용하면 DNS 요청이 Permit 규칙과 일치하지 않을 수 있습니다. 대신, DNS 요청은 후속 규칙에 대해 평가되며, 궁극적으로 전역 블록에 의해 차단될 수 있다.

예를 들어, 정책은 다음과 같이 구성될 수 있습니다.

1. Permit — DNS 트래픽/모든 대상
2. 거부 — 모든 프로토콜/모든 대상

이 컨피그레이션에서는 DNS 트래픽이 의도된 허용 규칙과 일치하지 않으며 후속 Deny Any/Any 규칙에 의해 차단될 수 있습니다.

왜 이것이 혼란스러울까요

Cisco Secure Access를 통해 관리자는 다음과 같은 애플리케이션 프로토콜을 선택할 수 있습니다.

- DNS
- DNS over HTTPS(DoH)
- DNS over TLS(DoT)

인터넷 액세스 정책 규칙을 구성할 때

따라서 DNS 트래픽은 애플리케이션 프로토콜 조건을 사용하여 항상 독립적으로 허용되거나 거부될 수 있습니다. 그러나 DNS 트래픽은 특정 정책 평가 동작의 영향을 받으며, 이 규칙 컨피그레이션에서 애플리케이션 프로토콜 또는 서비스 기반 조건(서비스 개체)을 예상대로 평가하지 못할 수 있습니다.

환경

- 이 문제는 다음과 같은 환경에 적용됩니다.
  - Cisco SSE(Secure Access)
  - 여러 규칙이 포함된 인터넷 액세스 정책
  - 프로토콜/애플리케이션 기반 규칙과 최종 Deny Any/Any 규칙의 조합
  - 선행 허용 규칙과 일치해야 하지만 대신 후속 규칙 또는 전역 블록에 의해 차단된 DNS 트래픽

해결

현재 이 정책 구조에서 Deny Any/Any 규칙이 뒤따를 때 Permit Any/Any DNS 규칙이 DNS 트래픽과 독립적으로 일치함을 보장하는 지원되는 컨피그레이션이 없습니다.

고객은 최종 Deny Any/Any 규칙이 포함된 인터넷 액세스 정책을 설계할 때 이 정책 평가 제한 사항에 유의해야 합니다.

DNS 트래픽을 허용해야 하는 경우, 평가 중인 DNS 트래픽에 적용할 수 있는 지원되는 규칙 조건을 사용하여 정책을 설계해야 합니다.

원인

DNS 트래픽은 일반 애플리케이션 트래픽과 같은 방식으로 서비스 기반 조건에 대해 평가되지 않습니다.

정책 규칙에 평가 중인 DNS 트래픽에 적용할 수 없는 조건이 포함된 경우 규칙이 일치하지 않습니다. 그런 다음 정책 평가는 적용 가능한 다음 규칙으로 계속 진행됩니다.

예를 들면 다음과 같습니다.

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

따라서 Permit DNS 규칙을 Deny Any/Any 규칙 바로 위에 배치한다고 해서 DNS 트래픽이 허용된다는 보장은 없습니다.

관련 콘텐츠

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.