FTD 액세스 제어 정책의 하위 도메인과 일치하지 않는 기본 도메인으로 FQDN 개체 트러블슈팅 (&N)

목차

문제

Cisco FTD(Firewall Threat Defense) 액세스 제어 정책에서 FQDN(Fully Qualified Domain Name) 개체를 구성할 때 기본 도메인 항목이 자동으로 하위 도메인과 일치하지 않습니다. 예를 들어 "example.com"으로 구성된 대상 개체를 허용하는 정책을 만들면 하위 도메인 "maps.example.com"은 동일한 정책 규칙을 통해 허용되지 않고 차단됩니다. 이러한 동작으로 인해 기본 도메인이 모든 하위 도메인에 대해 와일드카드로 작동할 수 있는지, 그리고 FTD 정책에서 와일드카드 FQDN 일치를 구현하기 위한 올바른 컨피그레이션 방법이 무엇인지에 대한 질문이 제기됩니다.

환경

- FTD 버전 7.2. 다른 버전도 영향을 받을 수 있습니다.
- FMC 버전 7.2. 다른 버전도 영향을 받을 수 있습니다.
- 액세스 제어 정책에 구성된 FQDN 객체

해결

- 관찰된 동작은 FQDN 객체의 예상 동작입니다.
- Cisco FMC에서 FQDN 객체는 정확한 도메인 이름과 일치하도록 설계되며 하위 도메인에 대한 와일드카드로 자동으로 작동하지 않습니다.
- 하위 도메인 매칭을 제대로 구성하려면 FQDN 개체 대신 URL 필터링 및 URL 조건을 사용해

야 합니다.

하위 도메인 매칭을 위한 URL 필터링 구성

FMC에서 도메인과 모든 하위 도메인을 일치시키려면 다음 컨피그레이션 단계를 수행합니다.

1단계. 액세스 제어 정책 규칙 컨피그레이션으로 이동합니다.

FMC에서 Policies(정책) > Access Control(액세스 제어) > Access Control Policy(액세스 제어 정책) > [Your Policy Name](정책 이름) > Rules(규칙)로 이동합니다.

2단계. 액세스 제어 규칙 생성 또는 편집

하위 도메인 일치를 구현하려는 경우 새 규칙을 생성하거나 기존 액세스 제어 규칙을 수정합니다.

3단계. URL 조건 구성

규칙 컨피그레이션에서 FQDN 객체를 사용하는 대신 URL 조건을 추가합니다. 하위 도메인과 일치하는 적절한 와일드카드 구문을 사용하여 기본 도메인을 포함하도록 URL 조건을 구성합니다.

4단계. URL 필터링 정책 적용

URL 필터링이 활성화되고 액세스 제어 정책 내에서 올바르게 구성되어 URL 조건을 효과적으로 처리하는지 확인합니다.

5단계. 컨피그레이션 구축

하위 도메인 일치 기능을 구현하기 위해 대상 FTD 디바이스에 컨피그레이션 변경 사항을 구축합니다.

대체 컨피그레이션 방법

URL 필터링이 특정 활용 사례에 적합하지 않은 경우 명시적으로 일치해야 하는 각 하위 도메인에 대해 여러 FQDN 객체를 생성하거나, 도메인이 예측 가능한 IP 주소 공간으로 확인되는 경우 IP 주소 범위의 네트워크 객체를 사용하는 것이 좋습니다.

원인

Cisco FMC의 FQDN 객체는 와일드카드 일치 대신 정확한 도메인 이름 일치를 수행하도록 설계되었습니다. 이는 시스템의 의도된 동작입니다. FQDN 개체 기능에는 암시적 하위 도메인 일치 기능이 포함되어 있지 않습니다. 이 기능을 사용하려면 원하는 하위 도메인 일치 동작을 달성하기 위해 URL 필터링 조건을 사용해야 합니다.

관련 콘텐츠

- 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
- Cisco 버그 ID CSCwf000588
- Cisco 기술 지원 및 다운로드

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.