

CSF에서 URL 범주 문제 해결 및 확인

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[관련 제품](#)

[배경 정보](#)

[아키텍처](#)

[1단계: FMC에서 URL 범주 조회](#)

[2단계: URL 필터링 통합 설정 검토](#)

[3단계: 시스템 지원 추적을 사용하여 디바이스의 URL 범주 확인](#)

[4단계: 범주 번호를 범주 이름으로 해결](#)

[다음을 확인합니다.](#)

[분쟁 버튼](#)

[문제 해결](#)

소개

이 문서에서는 디바이스에서 동일한 URL 분류를 사용하고 있는지 확인하기 위해 보안 방화벽 및 FMC에서 URL 범주 할당을 확인하는 방법에 대해 설명합니다.

사전 요구 사항

디바이스에 대해 활성화된 URL 필터링 라이선스, 정상 상태의 클라우드 서비스 통합, URL 필터링을 포함하며 URL 조건이 구성된 후 구축된 액세스 제어 정책이 있어야 합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(firepower 관리 센터) URL 필터링 및 범주 조회
- Cisco CSF(Secure Firewall) 트래픽 검사 및 정책 평가
- CSF 버전 6.5부터 시작되는 Talos를 기반으로 하는 URL 분류 및 평판 동작

사용되는 구성 요소

이 문서에서는 Cisco Secure Firewall 및 FMC 버전 6.5 이상에서 사용할 수 있는 기능에 대해 설명합니다. 이 설명서의 예에서는 버전 7.6.5를 사용합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 다음 제품 및 버전에도 사용할 수 있습니다.

- FMC(Secure Firewall Management Center)
- Cisco CSF(Secure Firewall)
- URL 필터링 및 클라우드 서비스 통합

배경 정보

URL 필터링은 트래픽 검사 중에 평가되는 카테고리 데이터베이스에 의존합니다. FMC는 대상에 대한 URL 카테고리 정보를 저장하며, 디바이스는 트래픽을 검사할 때 런타임 조회를 수행합니다. FMC, 디바이스 또는 클라우드 데이터베이스 간에 불일치가 있는 경우 액세스 제어 정책이 올바르게 구성된 경우에도 정책 결과가 일치하지 않을 수 있습니다.

검증에서 중요한 부분은 URL 카테고리 할당이 FMC와 디바이스 전체에서 일치하는지 확인하는 것입니다. URL 범주 조회는 클라우드 서비스 통합 설정 및 디바이스 캐시의 영향을 받습니다. 캐시 새로 고침 설정을 사용하지 않거나 항목 수명이 너무 길면 Talos가 분류를 업데이트한 후에도 오래된 범주 데이터가 계속 사용될 수 있습니다.

아키텍처

URL 필터링이 활성화된 경우 디바이스는 먼저 로컬 URL 캐시를 확인합니다. 카테고리가 캐시에 없는 경우 디바이스는 로컬 데이터베이스 또는 Cisco Cloud에 쿼리할 수 있습니다. 디바이스는 검사 중에 로컬 URL 데이터베이스 및 조회 캐시를 사용하며, 비커드는 Talos와 통신하여 URL 필터링 데이터를 다운로드하고 업데이트합니다. FMC 관리 디바이스에서 비커드는 FMC에서 실행되며 CSF에서 대기 상태에 있습니다. CSF가 로컬에서 관리되는 경우 프로세스는 디바이스 자체에서 실행됩니다.

Talos는 /var/sf/cloud_download/cisco에 저장된 다양한 크기의 전체 데이터베이스 패키지를 전송합니다.

다음은 Talos의 데이터베이스 파일이 어떤 형태인지 보여주는 몇 가지 예입니다.

- cisco_uridb_large_1541554243(500MB)
- cisco_uridb_medium_1541553645(125MB)
- cisco_uridb_small_1541553061(33MB)



참고: 데이터베이스 파일은 cisco_uridb로 시작하고 크기가 나열됩니다(small, medium 또는 large). 크기는 사용하는 하드웨어에 따라 달라질 수 있습니다.

1단계: FMC에서 URL 범주 조회

FMC는 URL 대상을 할당된 범주에 매핑하는 로컬 URL 데이터베이스를 유지 관리합니다. 이는 URL이 어떻게 분류되는지 검증할 때 권장되는 첫 번째 단계입니다.

FMC에서 Location Analysis > Advanced > URL로 이동합니다.

조사할 URL을 입력하고 할당된 카테고리를 검토합니다.

아래에 표시된 예에서 www.cisco.com는 Computers and Internet 카테고리 아래에 나열됩니다.

URL	Category	Reputation
www.cisco.com	Computers and Internet	Trusted

2단계: URL 필터링 통합 설정 검토

URL Filtering 통합 설정은 FMC 및 CSF 디바이스가 URL 카테고리 데이터베이스를 소싱할 위치를 결정합니다. 각 디바이스는 URL 조회를 위해 자체 로컬 데이터베이스를 유지 관리하며 Cisco

Cloud에 추가 또는 업데이트된 URL 인텔리전스를 쿼리할 수 있습니다.

FMC에서 Integration(통합) > Other Integrations(기타 통합) > Cloud Services(클라우드 서비스)로 이동하여 이러한 설정을 검토합니다.

URL Filtering

Last URL Filtering Update: 2026-08-26 10:28:52 [Update Now](#)

☒ Enable Automatic Updates

URL Query Source

☐ Local Database Only

☒ Local Database and Cisco Cloud

☐ Cisco Cloud Only

Cached URLs Expire

After 2 hours

[Dispute URL categories and reputations](#)

Save

통합이 정상적이고 URL 조회 캐시가 예상 정책 타이밍에 따라 새로 고치도록 구성되어 있는지 확인합니다.



주의: URL 조회 캐시는 이전에 검색된 카테고리 및 평판 결과를 유지할 수 있습니다. 캐시 만료가 비활성화되거나 수명이 긴 상태로 구성된 경우, Talos가 분류를 업데이트한 후 디바이스는 캐시된 정보를 계속 사용할 수 있으며, 이로 인해 디바이스 결과가 현재 FMC 또는 Talos 조회와 일시적으로 다를 수 있습니다.

3단계: 시스템 지원 추적을 사용하여 디바이스의 URL 범주 확인

CSF 디바이스가 FMC와 동일한 방법으로 URL을 분류하는지 확인하려면 디바이스 CLI에서 시스템 지원 추적을 실행합니다. 이는 Snort 검사 엔진이 트래픽을 평가하는 방법 및 연결을 검사할 때 반환되는 URL 범주를 보여줍니다.

FTD CLI에서 system support trace 명령을 입력하고 대화형 프롬프트에 응답합니다.

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 173.37.145.84
Please specify a server port: 443
```



참고: 이 예에서 173.37.145.84는 www.cisco.com의 IP 주소입니다. 조사 중인 URL에 해당하는 대상 IP 주소를 사용합니다.

출력 예:

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1: returned from url lookup, url_info is 90 2003
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1 URL lookup for www.cisco.com/ found rep 90, 2003
```

이 출력에서 URL은 카테고리 ID 2003을 반환합니다. 다음 단계에서는 해당 숫자 값을 해당 범주 이름으로 확인하는 방법에 대해 설명합니다.

4단계: 범주 번호를 범주 이름으로 해결

디바이스에 대한 URL 카테고리 조회는 숫자 카테고리 ID를 반환합니다. 이 번호를 사람이 읽을 수 있는 범주 이름에 매핑하려면 디바이스에서 `aup_categories.json` 파일을 엽니다.

expert 모드의 CSF에서 `/var/sf/cloud_download/directory`로 이동합니다. 루트 사용자 모드인지 확인합니다.

범주 정의 파일을 엽니다.

```
root@firepower:/var/sf/cloud_download# less aup_categories.json
```

추적 출력에서 반환된 범주 ID를 검색합니다. 카테고리 2003의 예 항목:

```
{
  "id": 2003,
  "uuid": "abba9b63-bb10-4729-b901-2e2aa0f02003",
  "mnemonic": "comp",
  "name": "Computers and Internet",
  "type": "aup_cats",
  "state": "active"
}
```



참고: 범주 ID 번호는 모든 CSF 디바이스에서 일관됩니다. 동일한 숫자 ID는 모든 CSF 디바이스의 동일한 범주 이름에 매핑됩니다.

다음을 확인합니다.

1~4단계의 출력을 사용하여 URL 범주 할당이 디바이스의 FMC 데이터베이스와 Snort 엔진 간에 일치하는지 확인합니다.

이 예에서는 다음을 수행합니다.

- FMC 데이터베이스에는 www.cisco.com [가](#) Computers 및 Internet으로 나열됩니다.
- 디바이스 CLI는 범주 ID 2003을 반환하며, 이는 컴퓨터 및 인터넷에 매핑됩니다.

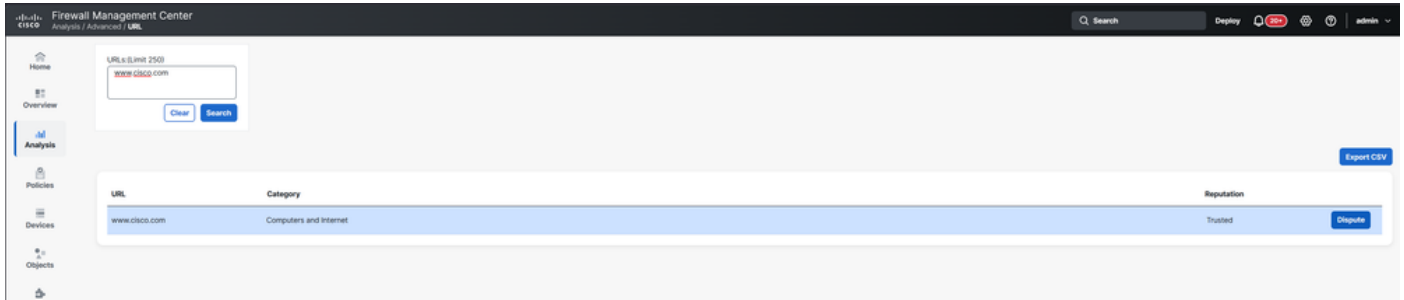
두 소스 모두 동의하며, 이는 적용 중인 URL 필터링 정책이 이 URL에 대해 일치함을 확인합니다.

분쟁 버튼

URL이 잘못된 카테고리로 분류되었다고 판단되면 Talos에 이의 제기를 제출할 수 있습니다.

FMC에서 Analysis > Advanced > URL로 이동합니다.

URL을 입력하고 검색을 클릭한 다음 URL 항목 위에 마우스를 놓고 Dispute를 선택합니다.



이렇게 하면 Talos 분쟁 페이지가 열리므로 적절한 출처에서 분류를 검토하고 수정할 수 있습니다.

문제 해결

분류가 예상과 일치하지 않으면 다음 영역을 검토하십시오.

- URL Filtering 라이선스가 활성화되어 있고 디바이스에 할당되어 있는지 확인합니다.
- 클라우드 서비스의 상태 및 Talos에 대한 연결을 확인합니다.
- 디바이스 캐시 및 캐시 새로 고침 설정을 검사하여 오래된 항목이 재사용되지 않는지 확인합니다.
- FMC 관리 디바이스에 대해 FMC에서 비커 프로세스가 실행 중인지 확인합니다.

FMC 관리 디바이스의 경우 FMC expert 모드에서 다음 명령을 실행하여 프로세스가 활성 상태인지 확인합니다.

```
pmtool status | grep beakerd
```



참고: FMC에서 관리하는 보안 방화벽에서 이 명령을 실행하면 프로세스가 대기 상태로 표시될 수 있습니다. Secure Firewall이 로컬에서 관리되는 경우 프로세스는 실행 중 상태로 표시됩니다.

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.