Firepower 데이터 경로 문제 해결 3단계: 보안 인텔리전스

목차

소개

이 문서는 Firepower 시스템의 데이터 경로 문제를 체계적으로 해결하여 Firepower의 구성 요소가 트래픽에 영향을 미치는지 여부를 확인하는 방법을 설명하는 일련의 문서 중 일부입니다. Firepower 플랫폼의 아키텍처에 대한 자세한 내용은 개요 문서를 참조하고 다른 데이터 경로 문제 해결 문서에 대한 링크를 참조하십시오.

이 문서에서는 Firepower 데이터 경로 문제 해결의 3단계인 보안 인텔리전스 기능을 다룹니다.

사전 요구 사항

- 이 문서는 현재 지원되는 모든 Firepower 플랫폼에 적용됩니다.
- URL 및 DNS에 대한 보안 인텔리전스가 버전 6.0.0에서 도입됨

Firepower 보안 인텔리전스 문제 해결 단계

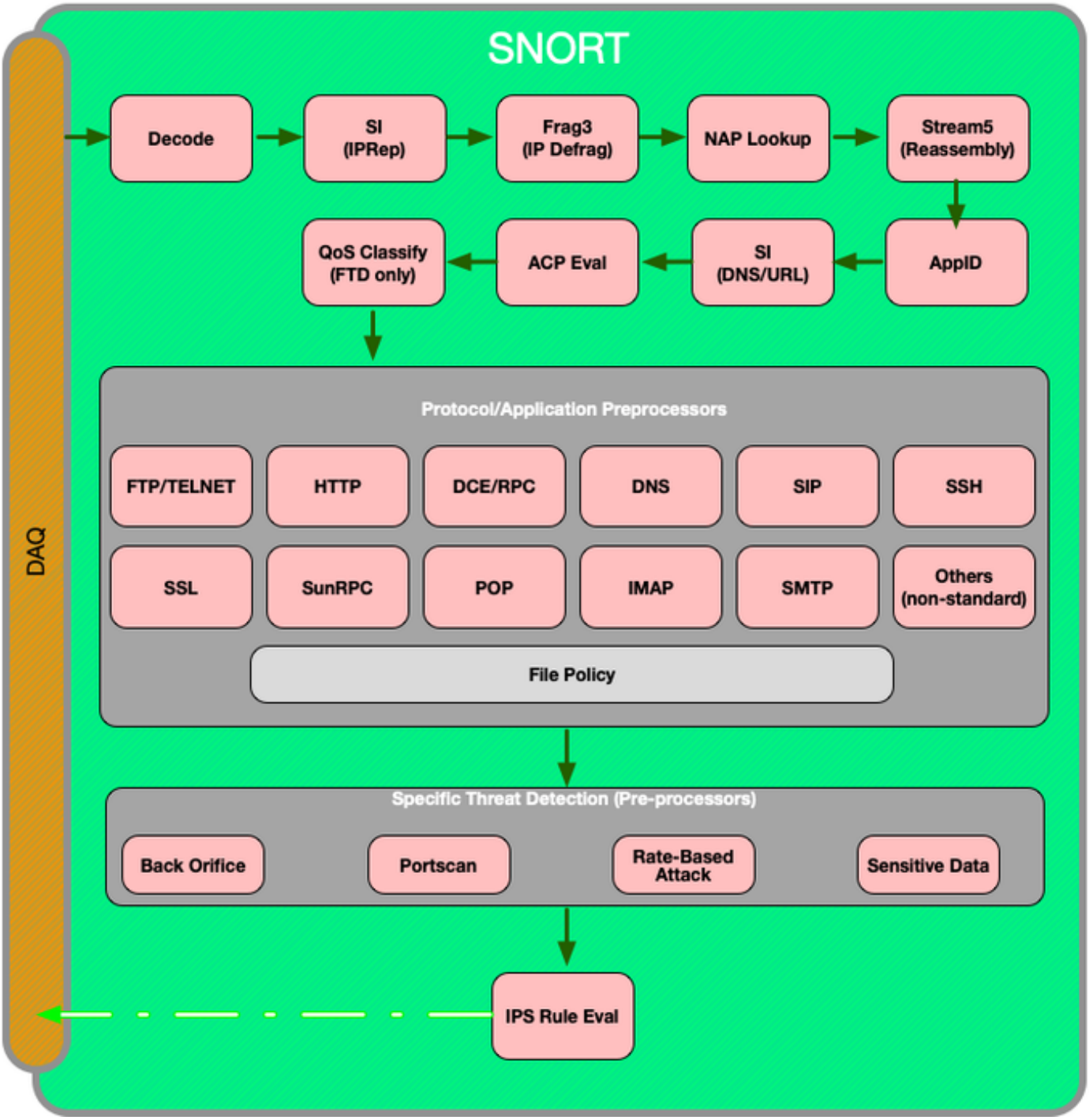
보안 인텔리전스는 블랙리스트와 화이트리스트 모두에서 다음 사항에 대해 검사를 수행하는 기능입니다.

- IP 주소(UI의 특정 부분에서는 "네트워크"라고도 함)
- URL(Uniform Resource Locator)
- DNS(Domain Name System) 쿼리

보안 인텔리전스 내의 목록은 시스코에서 제공하는 피드 및/또는 사용자가 구성한 목록과 피드로 채워질 수 있습니다.

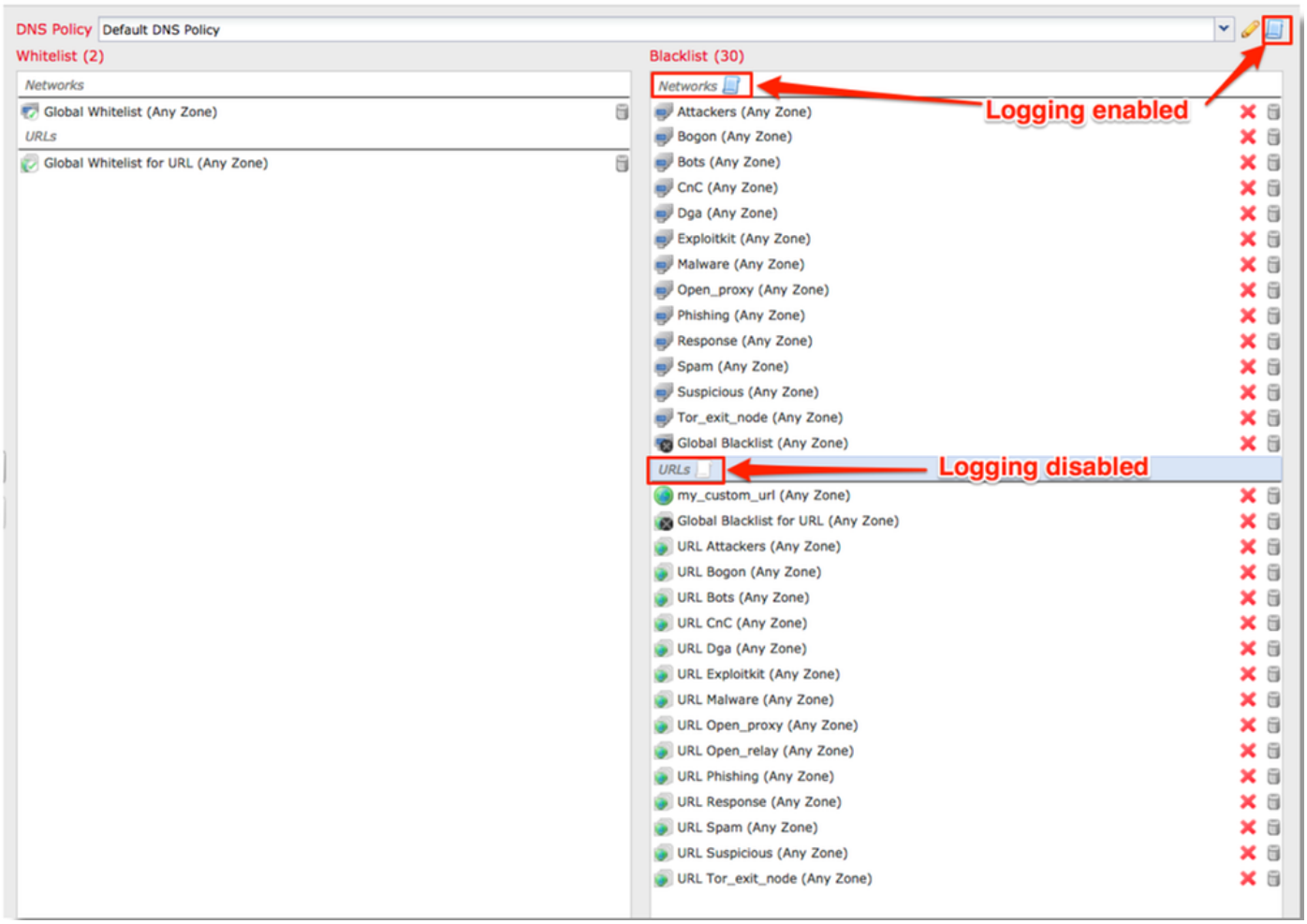
IP 주소를 기반으로 하는 보안 인텔리전스 평판은 트래픽을 검사하는 Firepower 내 첫 번째 구성 요

소입니다. URL 및 DNS 보안 인텔리전스는 관련 애플리케이션 프로토콜이 검색되는 즉시 수행됩니다. 다음은 Firepower 소프트웨어 검사 워크플로를 설명하는 다이어그램입니다.



보안 인텔리전스 이벤트에 대한 로깅이 활성화되었는지 확인

보안 인텔리전스 레벨의 차단은 로깅이 활성화되어 있는 한 쉽게 확인할 수 있습니다. 이는 **정책 > 액세스 제어 > 액세스 제어 정책**으로 이동하여 FMC(Firepower Management Center) UI(사용자 인터페이스)에서 확인할 수 있습니다. 해당 정책 옆에 있는 편집 아이콘을 클릭한 후 **보안 인텔리전스** 탭으로 이동합니다.

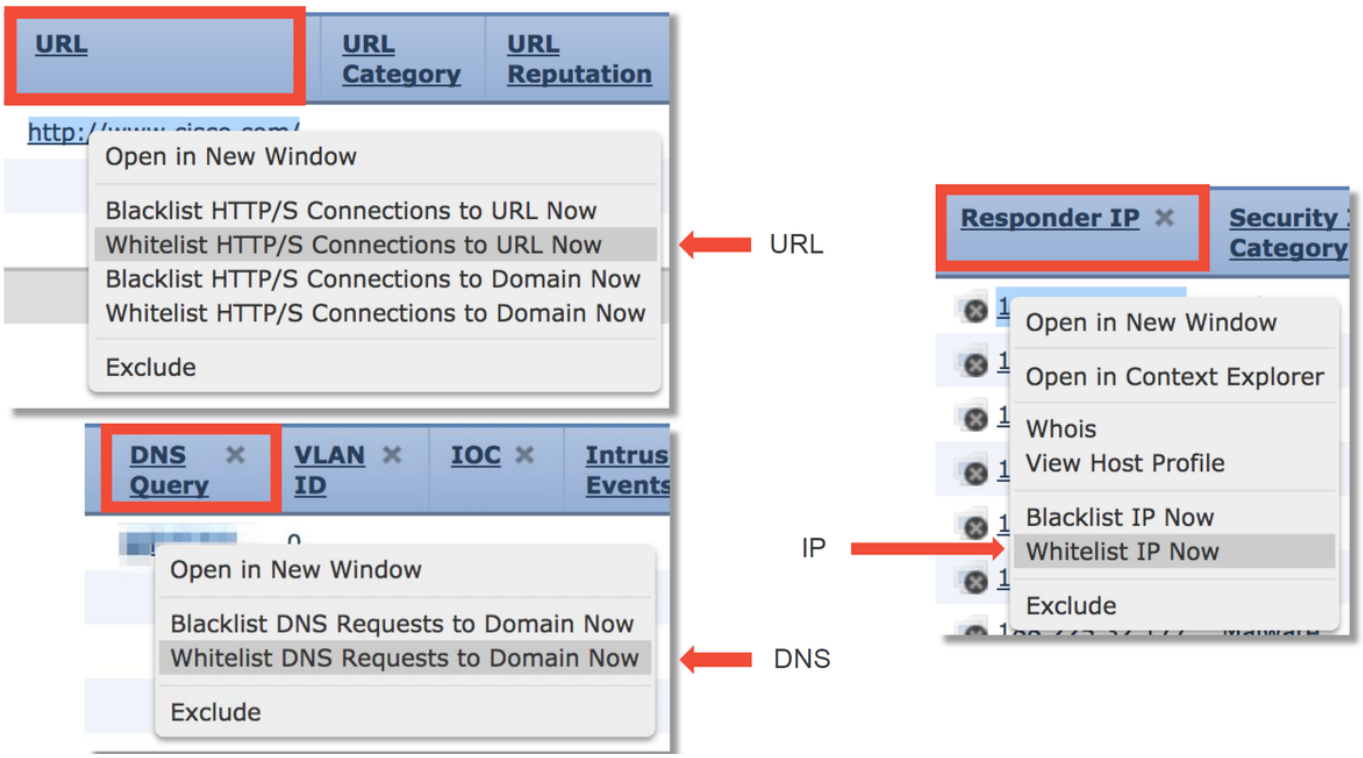


보안 인텔리전스 이벤트 검토

로깅이 활성화되어 있으면 **분석 > 연결 > 보안 인텔리전스 이벤트**에서 보안 인텔리전스 이벤트를 볼 수 있습니다. 트래픽이 차단되는 이유가 명확해야 합니다.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

빠른 완화 단계로, 보안 인텔리전스 기능에 의해 차단되는 IP, URL 또는 DNS 쿼리를 마우스 오른쪽 버튼으로 클릭하고 화이트리스트 옵션을 선택할 수 있습니다.



블랙리스트에 무언가 잘못 추가된 것으로 의심되거나 평판 변경을 요청하려는 경우 다음 링크에서 Cisco Talos를 사용하여 직접 티켓을 열 수 있습니다.

https://www.talosintelligence.com/reputation_center/support

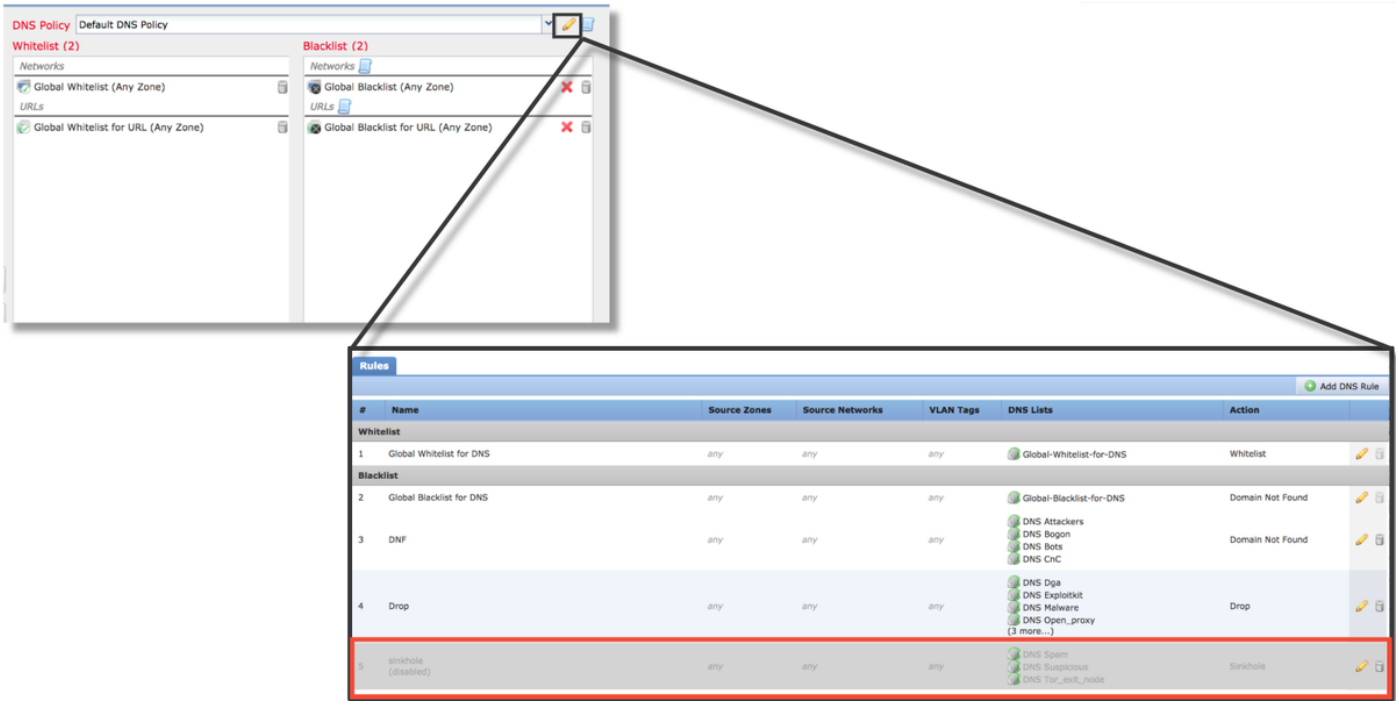
또한 블랙리스트에서 항목을 제거해야 하는지 여부를 조사하기 위해 Cisco TAC(Technical Assistance Center)에 데이터를 제공할 수 있습니다.

> **참고**: 화이트리스트에 추가하면 해당 보안 인텔리전스 화이트리스트에만 항목이 추가되며, 이는 개체가 보안 인텔리전스 검사를 통과할 수 있음을 의미합니다. 그러나 다른 모든 Firepower 구성 요소에서는 여전히 트래픽을 검사할 수 있습니다.

보안 인텔리전스 설정 제거 방법

보안 인텔리전스 설정을 제거하려면 위에서 설명한 대로 **보안 인텔리전스** 탭으로 이동합니다. 3개의 섹션, 즉 네트워크, URL, DNS 정책 섹션이 있습니다.

여기에서 휴지통 기호를 클릭하여 목록과 피드를 제거할 수 있습니다.



위의 스크린샷에서는 전역 블랙리스트 및 화이트리스트를 제외한 모든 IP 및 URL 보안 인텔리전스 목록이 제거된 것을 확인할 수 있습니다.

DNS 보안 인텔리전스 설정이 저장되는 DNS 정책 내에서 규칙 중 하나가 비활성화되어 있습니다.

> **참고**: 전역 블랙리스트 및 화이트리스트의 내용을 보려면 **개체 > 개체 관리 > 보안 인텔리전스**로 이동합니다. 그런 다음 원하는 섹션(네트워크, URL, DNS)을 클릭합니다. 목록을 편집하면 내용이 표시됩니다. 단, 설정은 액세스 제어 정책 내에서 수행해야 합니다.

백엔드의 설정 확인

보안 인텔리전스 설정은 **> show access-control-config** 명령을 통해 CLI에서 확인할 수 있습니다. 그러면 Firepower 디바이스에서 실행 중인 활성 액세스 제어 정책의 내용이 표시됩니다.

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
...[omitted for brevity]
```

위의 예에서는 네트워크 블랙리스트에 대해 로깅이 설정되어 있으며 블랙리스트에 최소 2개의 피드(Attackers 및 Bogon)가 포함되어 있습니다.

개별 항목이 보안 인텔리전스 목록에 있는지 여부는 전문가 모드에서 확인할 수 있습니다. 아래 단계를 참조하십시오.

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware



$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url



$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

IP SI lists are in /var/sf/iprep_download/

URL SI lists are in /var/sf/siurl_download/

DNS SI lists are in /var/sf/sidns_download/

각 보안 인텔리전스 목록에 대해 고유한 UUID의 파일이 있습니다. 위의 예에서는 **head -n1** 명령을

사용하여 목록의 이름을 식별하는 방법을 보여줍니다.

TAC에 제공할 데이터

데이터	지침
트래픽을 검사하는 FMC 및 Firepower 디바이스의 파일 문제 해결	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1176
이벤트 스크린샷(타임스탬프 포함)	지침은 이 문서를 참조하십시오.
CLI 세션의 텍스트 출력	지침은 이 문서를 참조하십시오.
오탐 사례를 제출하는 경우, 이의 제기할 항목(IP, URL, 도메인)을 제공합니다.	이의 제기를 수행해야 하는 이유 및 증거를 제공합니다.

다음 단계

보안 인텔리전스 구성 요소가 문제의 원인이 아닌 것으로 확인된 경우, 다음 단계로 액세스 제어 정책 규칙의 문제 해결을 수행합니다.

다음 문서로 이동하려면 여기를 클릭하십시오.

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.