FireSIGHT 시스템에서 URL 필터링 문제 해결

목차

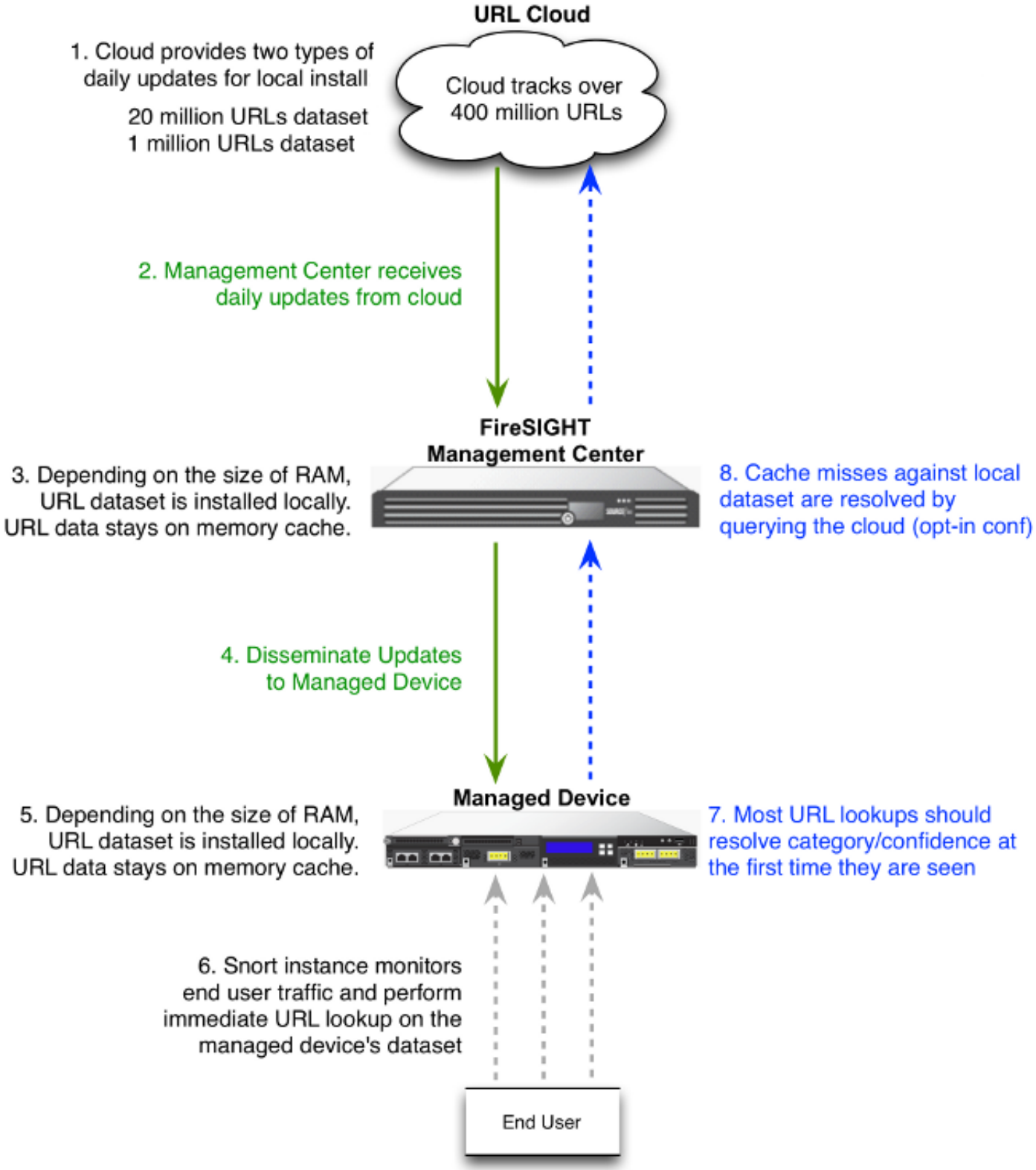
소개

이 문서에서는 URL 필터링의 일반적인 문제에 대해 설명합니다. FireSIGHT Management Center의 URL 필터링 기능은 모니터링되는 호스트의 트래픽을 분류하고 평판을 기반으로 액세스 제어 규칙에 조건을 작성할 수 있도록 합니다.

URL 필터링 조회 프로세스

URL 조회 프로세스를 가속화하기 위해 URL 필터링은 Firepower System에 로컬로 설치되는 데이터 집합을 제공합니다. 어플라이언스에서 사용 가능한 메모리(RAM)의 양에 따라 두 가지 유형의 데이터 세트가 있습니다.

데이터 집합 유형	메모리 요구 사항	
	버전 5.3	버전 5.4 이상
2,000만 URL 데이터 집합	>2GB	>3.4GB
1백만 URL 데이터 집합	<= 2GB	<= 3.4GB



클라우드 연결 문제

1단계: 라이센스 확인

라이센스가 설치되었습니까?

URL 필터링 라이센스가 없는 액세스 제어 규칙에 카테고리 및 평판 기반 URL 조건을 추가할 수 있지만, 먼저 FireSIGHT Management Center에 URL 필터링 라이센스를 추가한 다음 정책 대상 디바이스에서 활성화해야 액세스 제어 정책을 적용할 수 있습니다.

라이센스가 만료되었습니까?

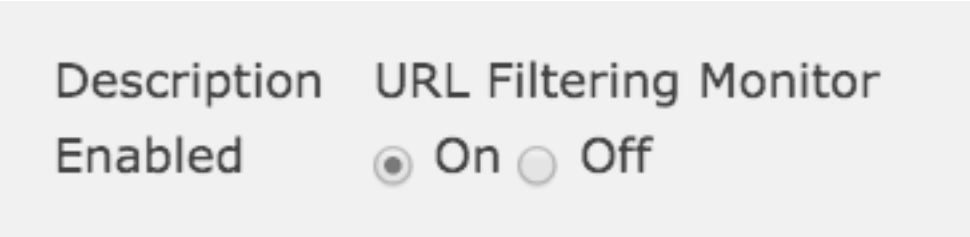
URL Filtering 라이센스가 만료되면 카테고리 및 평판 기반 URL 조건의 액세스 제어 규칙이 URL 필터링을 중지하며, FireSIGHT Management Center에서 더 이상 클라우드 서비스에 연결하지 않습니다.

> **팁:** FireSIGHT System에서 URL 필터링 기능을 활성화하고 관리되는 디바이스에 URL 필터링 라이센스를 적용하는 방법을 알아보려면 FireSIGHT System 컨피그레이션 예의 URL 필터링을 읽어보십시오.

2단계: 상태 알림 확인

URL Filtering Monitor 모듈은 FireSIGHT Management Center와 Cisco 클라우드 간의 통신을 추적합니다. 시스템에서는 자주 방문하는 URL에 대한 URL 필터링(카테고리 및 평판) 데이터를 가져옵니다. URL Filtering Monitor 모듈은 FireSIGHT Management Center와 URL 필터링을 활성화한 관리되는 디바이스 간의 통신도 추적합니다.

URL Filtering Monitor 모듈을 활성화하려면 **Health Policy** Configuration 페이지로 이동하여 **URL Filtering Monitor**를 선택합니다. 상태 테스트를 위해 **모듈**의 사용을 **활성화하려면** Enabled 옵션에 대한 On 라디오 버튼을 클릭합니다. 설정을 적용하려면 FireSIGHT Management Center에 상태 정책을 적용해야 합니다.



- **중요 알림**: FireSIGHT Management Center가 클라우드와 성공적으로 통신하거나 클라우드에서 업데이트를 검색하지 못하면 해당 모듈에 대한 상태 분류가 Critical로 *변경됩니다*.
- **경고 알림**: FireSIGHT Management Center가 클라우드와 성공적으로 통신할 경우 Management Center가 관리되는 디바이스에 새 URL 필터링 데이터를 푸시할 수 없으면 모듈 상태가 *Warning*(경고)으로 변경됩니다.

3단계: DNS 설정 확인

FireSIGHT Management Center는 클라우드 조회 중에 다음 서버와 통신합니다.

```
database.brightcloud.com
service.brightcloud.com
```

방화벽에서 두 서버가 모두 허용되는지 확인한 후 FireSIGHT Management Center에서 다음 명령을 실행하고 Management Center에서 이름을 확인할 수 있는지 확인합니다.

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.com

admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

4단계: 필수 포트에 대한 연결 확인

FireSIGHT 시스템은 클라우드 서비스와 통신하기 위해 포트 443/HTTPS 및 80/HTTP를 사용합니다.

Management Center에서 성공적으로 nslookup을 수행할 수 있는지 확인했으면 텔넷을 사용하여 포트 80 및 포트 443에 대한 연결을 확인합니다. URL 데이터베이스는 포트 443에서 database.brightcloud.com과 함께 다운로드되며, 알 수 없는 URL 쿼리는 포트 80의 service.brightcloud.com에서 수행됩니다.

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

이 출력은 database.brightcloud.com에 대한 텔넷 연결에 성공한 예입니다.

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

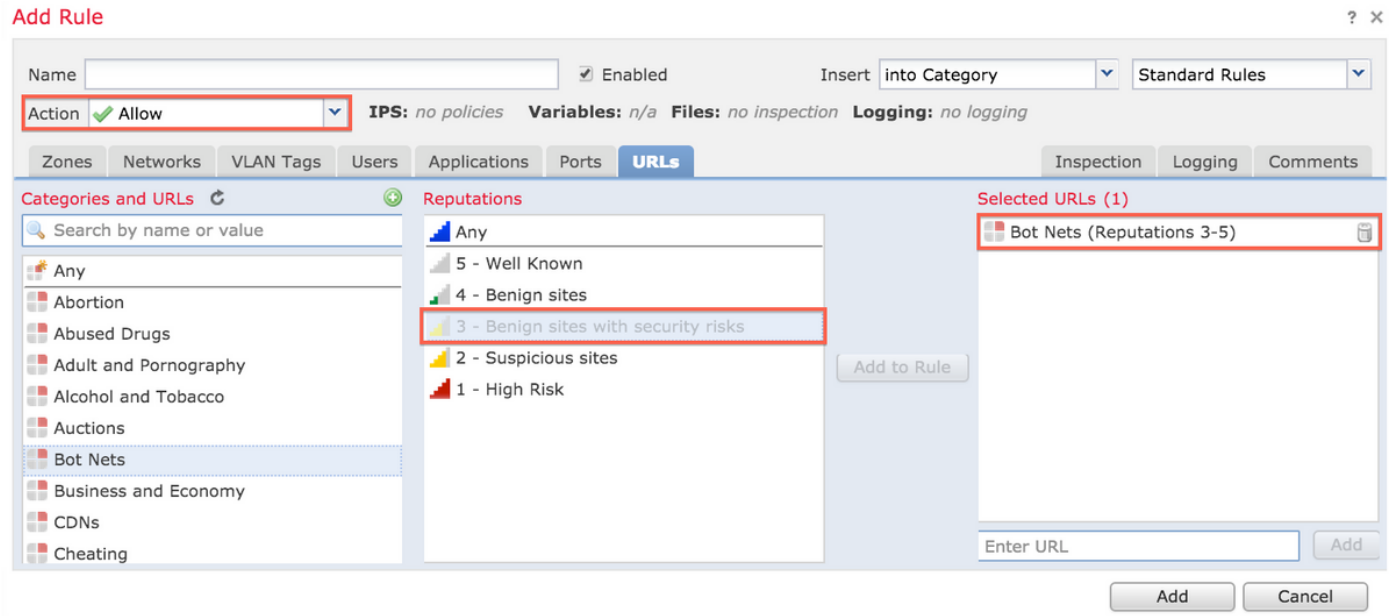
액세스 제어 및 잘못된 분류 문제

문제 1: 선택되지 않은 평판 수준의 URL이 허용/차단됨

URL이 허용되거나 차단되었지만 액세스 제어 규칙에서 해당 URL의 평판 수준을 선택하지 않은 경우 URL 필터링 규칙이 작동하는 방식을 이해하려면 이 섹션을 읽어 보십시오.

규칙 작업이 허용임

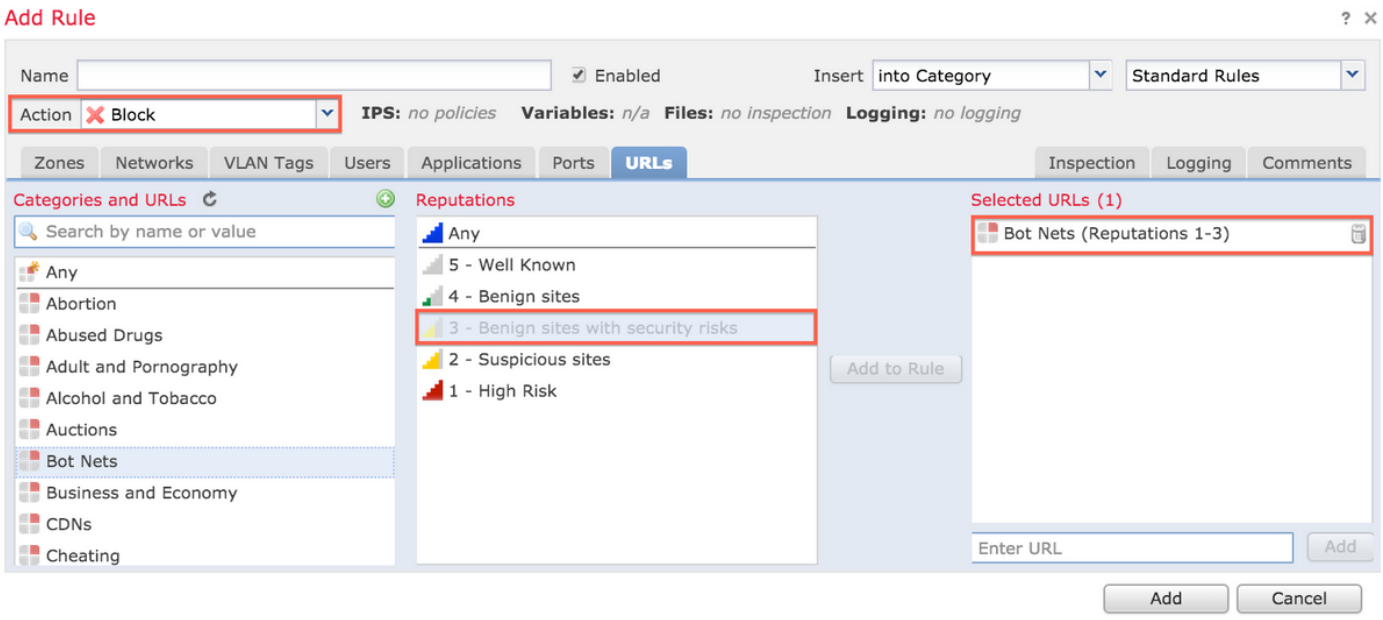
평판 레벨을 기반으로 **트래픽**을 허용하는 규칙을 생성할 때, 평판 레벨을 선택하면 원래 선택한 레벨보다 안전하지 않은 모든 평판 레벨이 선택됩니다. 예를 들어, *보안 위험*이 있는 *양성 사이트*(수준 3)를 허용하는 규칙을 구성할 경우, *양성 사이트*(수준 4) 및 *잘 알려진*(수준 5) 사이트도 자동으로 허용합니다.



규칙 작업이 차단됨

평판 레벨을 기반으로 **트래픽**을 차단하는 규칙을 생성할 때, 평판 레벨을 선택하면 원래 선택한 레벨보다 심각한 모든 평판 레벨이 선택됩니다. 예를 들어 *보안 위험*이 있는 *양성 사이트*(수준 3)를 차

단하는 규칙을 구성할 경우 *의심스러운 사이트*(수준 2) 및 *높은 위험*(수준 1) 사이트도 자동으로 차단됩니다.



URL 선택 매트릭스

선택한 평판 수준 **1 - 고위험** **2 - 의심스러운 사이트** **3 - 보안 위험이 있는 안전한 사이트** **4 - 안전한 사이트** **5 - 잘 알려진**	선택한 규칙 작업 **고위험**	**의심스러운 사이트**	**보안 위험이 있는 안전한 사이트**	**양성 사이트**	**주**
	,	,	,	,	,

문제 2: 와일드카드가 액세스 제어 규칙에서 작동하지 않음

FireSIGHT 시스템은 URL 조건에서 와일드카드 지정을 지원하지 않습니다. 이 조건은 cisco.com에서 알림을 보내지 못할 수 있습니다.

```
*cisco*.com
```

또한 불완전한 URL이 다른 트래픽과 일치하여 원하지 않는 결과가 발생할 수 있습니다. URL 조건에서 개별 URL을 지정할 때 영향을 받을 수 있는 다른 트래픽을 신중하게 고려해야 합니다. 예를 들어, cisco.com을 명시적으로 차단하려는 시나리오를 가정해보겠습니다. 그러나 하위 문자열 매칭은 cisco.com을 차단하면 sanfrancisco.com도 차단됩니다. 이는 의도한 바가 아닐 수 있습니다.

URL을 입력할 때 도메인 이름을 입력하고 하위 도메인 정보를 생략합니다. 예를 들어, www.cisco.com이 아닌 cisco.com을 입력합니다. Allow(허용) 규칙에서 cisco.com을 사용할 경우 **다음** URL 중 하나로 이동할 수 있습니다.

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

문제 3: URL 범주 및 평판이 채워지지 않음

URL이 로컬 데이터베이스에 없고 URL이 트래픽에서 처음으로 표시되는 경우, 카테고리 또는 평판이 채워지지 않을 수 있습니다. 즉, 알 수 없는 URL이 처음 표시될 때 AC 규칙과 일치하지 않습니다. 일반적으로 방문하는 URL에 대한 URL 조회는 URL을 처음 볼 때 확인되지 않을 수 있습니다. 이 문제는 버전 5.3.0.3, 5.3.1.2 및 5.4.0.2, 5.4.1.1에서 수정되었습니다.

관련 정보

- FireSIGHT 시스템에서 URL 필터링 컨피그레이션
- 기술 지원 및 문서 – Cisco Systems