웹 보호

웹 애플리케이션 방화벽(WAF)

웹 보호 프로파일은 트래픽이 악의적이지 않은지 확인하기 위해 웹 기반 트랜잭션을 평가하는 데 사용할 수 있는 WAF(Web Application Firewall) 규칙 모음입니다.

사용자 지정 WAF 규칙 업로드

멀티 클라우드 방어에서는 다음 WAF 규칙 집합을 지원합니다.

Table 1: 멀티 클라우드 방어에서는 다음 ***WAF*** 규칙 집합을 지원합니다.

규칙 집합	설명
핵심 규칙	핵심 규칙은 모든 웹 애플리케이션에 기본 보호 레벨을 제공하는 ModSecurity CRS(핵심 규칙 집합)의 표준 규칙 집합입니다.
TrustWave 규칙	TrustWave 규칙은 특정 웹 애플리케이션 및 프레임워크에 고급 수준의 보호를 제공하는 실제 조사, 침입 테스트 및 연구를 통해 수집된 인텔리전스를 기반으로 하는 ModSecurity의 고급 규칙 집합입니다.
사용자 지정 규칙	사용자 지정 규칙은 맞춤형 웹 애플리케이션에 특수 수준의 보호를 제공하며 고객이 작성한 특정 규칙 집합입니다.

하나 이상의 규칙을 포함하는 사용자 지정 규칙 규칙 집합은 멀티 클라우드 방어 WAF 보안 엔진에서 업로드되어 사용될 수 있습니다. 규칙 집합에 포함된 규칙은 특정 웹 애플리케이션 및 프레임워크에 대해 고객이 필요로 하는 특수 웹 애플리케이션 평가를 제공합니다. WAF 프로파일에 구성된 다른 규칙 집합을 평가하기 전에 WAF 프로파일에 포함된 사용자 지정 규칙을 먼저 평가합니다.

사용자 지정 규칙 규칙 집합을 업로드할 경우 파일은 확장자가 tar.gz인 Gzip 압축 TAR 파일이어야 합니다. 압축된 TAR 파일은 다음 파일로 구성됩니다.

- Readme 파일 - 규칙 집합의 설명을 제공하는 파일입니다.
- 변경 로그 파일 - 변경 기록을 나타내는 파일입니다.
- 규칙 폴더 - 하나 이상의 ModSecurity 형식의 규칙 파일로 구성된 폴더입니다. 각 파일에는 확장자.conf가 있어야 합니다. 폴더는 하나 이상의 규칙 파일을 포함해야 합니다(비워둘 수 없음). 각 파일은 ModSecurity 규칙 형식 지침을 따라야 합니다.

단계 **1** **Manage(**관리**)** > **Threat Research(**위협 연구**)** > **Web Protection(**웹 보호**)**으로 이동합니다.

단계 **2** **Custom(**사용자 지정**)** 탭을 클릭합니다.

단계 **3** **Import(**가져오기**)** 버튼을 클릭하고 사용자 지정 규칙 집합 파일을 업로드합니다.

WAF 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Web Protection(**웹 보호**)**으로 이동합니다.

단계 **2** **Create Protection Profile(**보호 프로파일 생성**)** > **Application Threat(**애플리케이션 위협**)**을 클릭합니다.

단계 **3** 다음 일반 설정을 지정합니다.

a) 프로파일 이름 및 설명을 지정합니다.

b) 작업을 지정합니다.

- **Rule Default(**규칙 기본값**)** - 트리거된 각 규칙에 지정된 작업에 따라 요청을 허용하거나 거부하고 이벤트를 로깅합니다.
- **Allow Log(**로그 허용**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Deny Log(**로그 거부**)** - 요청을 거부하고 이벤트를 로깅합니다.

c) WF 프로파일이 악의적인 활동을 탐지하는 경우, 위협 HAR 파일을 생성할지 여부를 지정합니다.

d) WAF 프로파일이 악의적인 활동을 탐지하는 경우 HTTP 요청 HAR 파일을 생성할지 여부를 지정합니다.

e) WAF 프로파일의 규칙 라이브러리(Core, TrustWave, Custom)에서 하나 이상의 규칙 집합을 지정해야 합니다. Core Rules(핵심 규칙)를 지정합니다.

1. **Manual(**수동**)** 또는 **Automatic(**자동**)**을 지정합니다.
   - **Manual(**수동**)** - 사용할 핵심 규칙 버전을 지정합니다.
   - **Automatic(**자동**)** - 게시 날짜로부터 최신 핵심 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.
2. 특정 핵심 규칙 규칙 집합을 WAF 프로파일에 추가합니다.

Note 핵심 규칙 규칙 집합이 지정된 경우, 핵심 규칙을 비활성화할 수 없습니다. 핵심 규칙을 비활성화하려면 WAF 프로파일에서 모든 핵심 규칙 규칙 집합을 제거하여 평가되지 않도록 합니다.

f) TrustWave 규칙을 지정합니다.

1. **Disabled(**비활성화됨**)**, **Manual(**수동**)**, **Automatic(**자동**)**을 지정합니다.
   - **Disabled(**비활성화됨**)** - TrustWave 규칙 사용을 비활성화할지 여부를 지정합니다(위의 기술 노트 참조).
   - **Manual(**수동**)** - 사용할 TrustWave 규칙 버전을 지정합니다.
   - **Automatic(**자동**)** - 게시 날짜로부터 최신 TrustWave Rules 버전으로의 자동 업데이트를 연기할 기간(일)을 지정합니다.
2. 특정 TrustWave 규칙 규칙 집합을 WAF 프로파일에 추가합니다.

Note TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 사용하는 경우 둘 중 하나 이상을 활성화해야 합니다. 두 가지를 모두 비활성화하려는 경우에는 WAF 프로파일에서 모든 TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 제거하여 평가되지 않도록 합니다.

g) Custom Rules(사용자 지정 규칙)를 지정합니다.

1. **Disabled(**비활성화됨**)**, **Manual(**수동**)**, **Automatic(**자동**)**을 지정합니다.
   - **Disabled(**비활성화됨**)** - 사용자 지정 규칙 사용을 비활성화할지 여부를 지정합니다(위의 기술 노트 참조).
   - **Manual(**수동**)** - 사용할 사용자 지정 규칙 버전을 지정합니다.
   - **Automatic(**자동**)** - 게시 날짜로부터 최신 사용자 지정 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.
2. 특정 사용자 지정 규칙 규칙 집합을 WAF 프로파일에 추가합니다.

Note TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 사용하는 경우 둘 중 하나 이상을 활성화해야 합니다. 두 가지를 모두 비활성화하려는 경우에는 WAF 프로파일에서 모든 TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 제거하여 평가되지 않도록 합니다.

Note 전체 WF 프로파일을 비활성화하려면 정책 규칙 집합 규칙에서 WAF 프로파일을 제거하여 WAF 프로파일이 평가되지 않습니다.

단계 **4** 다음 고급 설정을 지정합니다.

a) 규칙 삭제를 지정합니다. 특정 IP 또는 CIDR 목록에 대한 규칙을 억제할 수 있습니다.

1. **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.
2. Rule Suppression(규칙 억제)에서 **Add(**추가**)**를 클릭합니다.
3. **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)**에서 쉼표로 구분된 IP 또는 CIDR 목록을 제공합니다.
4. **Rule ID List(**규칙 **ID** 목록**)**에 쉼표로 구분된 규칙 ID 목록을 제공합니다.

b) WF 프로파일이 악의적인 활동을 탐지하는 경우, 위협 HAR 파일을 생성할지 여부를 지정합니다.
c) WAF 프로파일이 악의적인 활동을 탐지하는 경우 HTTP 요청 HAR 파일을 생성할지 여부를 지정합니다.
d) WAF 프로파일의 규칙 라이브러리(Core, TrustWave, Custom)에서 하나 이상의 규칙 집합을 지정해야 합니다. Core Rules(핵심 규칙)를 지정합니다.

1. **Manual(**수동**)** 또는 **Automatic(**자동**)**을 지정합니다.
   - **Manual(**수동**)** - 사용할 핵심 규칙 버전을 지정합니다.
   - **Automatic(**자동**)** - 게시 날짜로부터 최신 핵심 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.
2. 특정 핵심 규칙 규칙 집합을 WAF 프로파일에 추가합니다.

Note 핵심 규칙 규칙 집합이 지정된 경우, 핵심 규칙을 비활성화할 수 없습니다. 핵심 규칙을 비활성화하려면 WAF 프로파일에서 모든 핵심 규칙 규칙 집합을 제거하여 평가되지 않도록 합니다.

e) TrustWave 규칙을 지정합니다.

1. **Disabled(**비활성화됨**)**, **Manual(**수동**)**, **Automatic(**자동**)**을 지정합니다.
   - **Disabled(**비활성화됨**)** - TrustWave 규칙 사용을 비활성화할지 여부를 지정합니다(위의 기술 노트 참조).
   - **Manual(**수동**)** - 사용할 TrustWave 규칙 버전을 지정합니다.
   - **Automatic(**자동**)** - 게시 날짜로부터 최신 TrustWave Rules 버전으로의 자동 업데이트를 연기할 기간(일)을 지정합니다.
2. 특정 TrustWave 규칙 규칙 집합을 WAF 프로파일에 추가합니다.

Note TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 사용하는 경우 둘 중 하나 이상을 활성화해야 합니다. 두 가지를 모두 비활성화하려는 경우에는 WAF 프로파일에서 모든 TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 제거하여 평가되지 않도록 합니다.

f) Custom Rules(사용자 지정 규칙)를 지정합니다.

1. **Disabled(**비활성화됨**)**, **Manual(**수동**)**, **Automatic(**자동**)**을 지정합니다.
   - **Disabled(**비활성화됨**)** - 사용자 지정 규칙 사용을 비활성화할지 여부를 지정합니다(위의 기술 노트 참조).
   - **Manual(**수동**)** - 사용할 사용자 지정 규칙 버전을 지정합니다.
   - **Automatic(**자동**)** - 게시 날짜로부터 최신 사용자 지정 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.
2. 특정 사용자 지정 규칙 규칙 집합을 WAF 프로파일에 추가합니다.

Note TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 사용하는 경우 둘 중 하나 이상을 활성화해야 합니다. 두 가지를 모두 비활성화하려는 경우에는 WAF 프로파일에서 모든 TrustWave 규칙 및 사용자 지정 규칙 규칙 집합을 제거하여 평가되지 않도록 합니다.

이벤트 필터링

WAF 프로파일이 트리거될 때 생성되는 보안 이벤트 수를 줄이기 위해 이벤트 속도를 제한하거나 샘플링하도록 이벤트 필터링을 구성할 수 있습니다. 설정은 탐지 또는 보호 동작을 변경하지 않습니다.

Type(유형)을 **Rate(**속도**)**로 지정하면 생성되는 이벤트는 *Time(*시간*)* 평가 간격(초) 동안 트리거된 지정된 *Number of Events(*이벤트 수*)*에 따라 속도가 제한됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 50으로 지정되고 *Time(*시간*)*이 5초로 지정된 경우 초당 10개 이벤트만 생성됩니다.

Type(유형)을 **Sample(**샘플**)**로 지정하면 생성된 Events(이벤트)는 지정된 *Number of Events(*이벤트 수*)*를 기준으로 샘플링됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 10으로 지정된 경우, 트리거된 10개 이벤트마다 1개의 이벤트만 생성됩니다.

프로파일 이벤트 필터링

프로파일 이벤트 필터링은 WAF 프로파일에 설정된 모든 규칙에 적용됩니다.

- Type(유형)을 **Rate(**속도**)** 또는 **Sample(**샘플**)**로 지정합니다.
  - **Rate(**속도**)** - *Number of Events(*이벤트 수*)* 및 *Time(*시간*)* 평가 간격(초)을 지정합니다.
  - **Sample(**샘플**)** - *Number of Events(*이벤트 수*)*를 지정합니다.

규칙 이벤트 필터링

규칙 이벤트 필터링은 IDS/IPS 프로파일에 설정된 특정 규칙에 적용됩니다.

단계 **1** **Rule Event Filtering(**규칙 이벤트 필터링**)** 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **2** *Rule ID List(*규칙 *ID* 목록*)*에서 쉼표로 구분된 *Rule ID(*규칙 *ID)* 목록을 지정합니다.

단계 **3** Type(유형)을 *Rate(*속도*)* 또는 *Sample(*샘플*)*로 지정합니다.

- *Rate(*속도*)* - *Number of Events(*이벤트 수*)* 및 *Time(*시간*)* 평가 간격(초)을 지정합니다.
- *Sample(*샘플*)* - *Number of Events(*이벤트 수*)*를 지정합니다.

다음에 수행할 작업

이벤트 필터링 프로파일 연결

이 문서를 확인하여 규칙 생성/편집

L7 DoS 프로파일 생성

레이어 7 DoS 공격은 웹 서버 리소스를 고갈시키기 위한 것으로, 많은 HTTP 요청을 전송하여 서비스 가용성에 영향을 미칩니다. 멀티 클라우드 방어 게이트웨이에서 제공하는 기능을 사용하면 백엔드 웹 서버에 대한 클라이언트 요청을 지속적으로 모니터링하여 애플리케이션 레이어 공격을 모니터링, 탐지 및 치료할 수 있습니다. 이 기능은 백엔드 웹 서비스에 대한 인바운드 연결을 프록시하기 위해 게이트웨이를 활성화할 때 활성화됩니다. 또한 이 기능을 활성화하면 프런트엔드 로드 밸런서가 지원하지 않거나 애플리케이션 DoS 공격을 탐지하고 치료하도록 최적화되지 않은 경우에 게이트웨이에서 보안 수준을 추가할 수 있습니다.

이 기능은 백엔드 웹 서비스에 적용하여 웹 기반 애플리케이션의 가용성을 유지 관리할 수 있으며, API 서비스를 호스팅하는 백엔드 웹 서버에 대한 DoS 보호를 제공하는 데에도 사용할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Web Protection(**웹 보호**)**으로 이동합니다.

단계 **2** **Layer 7 DOS**를 선택합니다.

단계 **3** 이름과 설명을 제공합니다.

단계 **4** 요청 속도 제한을 추가합니다.

리소스에 대한 과도한 요청은 다음 매개변수를 기반으로 제한합니다. 이 매개변수의 값은 레이어 7 DOS 옵션으로 보호하려는 웹 서비스의 트래픽 패턴 측정 및 이해를 기반으로 해야 합니다.

Table 2: 매개변수

매개변수	설명
URI	리소스에 대한 요청을 제한하는 경로를 나타내는 데 사용되는 상대적 URI입니다. 예를 들어 https://www.example.com/login.html에서 서비스 리소스를 모니터링하고 보호하려는 경우 **Request Rate Limits(**요청 속도 제한**)** 테이블에 URI 매개변수로 /login.html을 입력합니다.
HTTP 메서드	리소스 URI당 HTTP 메서드를 지정하여 클라이언트 요청에서 속도가 제한되는 HTTP 메서드와 속도가 제한되지 않는 HTTP 메서드를 제어할 수 있습니다. 테이블의 각 행에 대해 드롭다운에서 여러 메서드를 선택할 수 있습니다. 빈 HTTP 메서드 목록은 메서드가 무시되고 속도가 리소스에 대한 모든 호출에 적용됨을 의미합니다. **Note** 속도는 리소스별로 적용됩니다. 따라서 여러 메서드가 해당 행의 요청 속도에 지정된 속도 제한을 공유합니다. 예를 들어 속도가 초당 3개 요청이고 GET, POST 및 PUT이 HTTP 메서드에 지정되어 있으며 동일한 시간(초)에 단일 클라이언트 IP에서 해당 URI에 2개의 GET과 1개의 POST가 발생하는 경우, 같은 초에 PUT은 허용되지 않습니다.
요청 속도	초당 요청 수입니다. 단일 클라이언트가 규칙의 URI 부분에 언급된 URI 리소스에 요청을 전송할 수 있는 속도를 결정합니다.

매개변수	설명
BurstSize	클라이언트가 규칙의 URI 부분에 언급된 URI 리소스에 전송할 수 있는 최대 동시 요청 수를 지정합니다. 이 임계값을 초과하며 동시에 프록시에 도착하는 요청은 백엔드 서버로 전송되지 않습니다.

단계 **5** 완료되면 **Save(**저장**)**를 클릭합니다.

Note 규칙은 위에서 아래로 확인되고 첫 번째 일치에 적용되므로 URI를 기준으로 하면 규칙의 순서가 중요합니다. 목록의 상위에 추가된 URI가 그 아래에 있는 규칙의 리소스를 포함하는 리소스 경로를 포함하는 경우, 일치하는 첫 번째 규칙이 적용됩니다.

Example

2개의 웹 서비스 리소스가 보호됩니다.

1. /login.html은 더 작은 속도와 버스트 크기로 제한되며, GET 및 POST 메서드 모두 위에 설명된 대로 속도를 공유합니다. 다른 모든 메서드는 속도 제한을 적용하지 않고 허용됩니다.
2. /index.html은 더 큰 속도와 버스트 크기로 제한되며, GET 호출만 속도가 제한됩니다.

What to do next

- 서비스 개체 연결

  레이어 7 DOS 보호 프로파일이 생성되면 리스너 및 백엔드 서버 주소에 대한 연결을 나타내는 ReverseProxy 서비스 개체와 연결되어야 합니다.

- **L7 DoS** 프로파일을 정책 규칙과 연결

  정책 규칙을 생성/편집하려면 이 문서를 확인합니다.