오탐 침입을 줄이기 위한 옵션

목차

소개

침입 방지 시스템은 특정 Snort 규칙에 대해 과도한 알림을 생성할 수 있습니다. 알림은 true positive 또는 false positive일 수 있습니다. 오탐 알림이 많이 발생하는 경우 이를 줄일 수 있는 몇 가지 옵션이 있습니다. 이 글에서는 각 옵션의 장단점을 요약하여 제공합니다.

오탐 알림 감소 옵션

> 참고: 일반적으로 이러한 옵션은 최선의 방법이 아니며 특정 상황에서 유일한 솔루션이 될 수 있습니다.

1. Cisco 기술 지원에 보고

정상적인 트래픽에 대한 알림을 트리거하는 Snort 규칙을 발견한 경우 이를 Cisco 기술 지원에 보고하십시오. 보고되면 고객 지원 엔지니어가 VRT(Vulnerability Research Team)로 문제를 에스컬레이션합니다. VRT는 규칙의 개선 가능성을 조사합니다. 개선된 규칙은 일반적으로 리포터가 사용 가능한 즉시 사용할 수 있으며, 다음 공식 규칙 업데이트에도 추가됩니다.

2. 신뢰 또는 허용 규칙

신뢰할 수 있는 트래픽이 검사 없이 Sourcefire 어플라이언스를 통과하도록 허용하는 가장 좋은 옵션은 관련 침입 정책 없이 Trust 또는 Allow 작업을 활성화하는 것입니다. Trust 또는 Allow 규칙을 구성하려면 Policies(정책) > Access Control(액세스 제어) > Add Rule(규칙 추가)로 이동합니다.

> 참고: 사용자, 애플리케이션 또는 URL과 일치하도록 구성되지 않은 Trust 또는 Allow 규칙은 Firepower 하드웨어에서 처리할 수 있으므로 Sourcefire 어플라이언스의 전체 성능에 미치는 영향이 최소화됩니다.

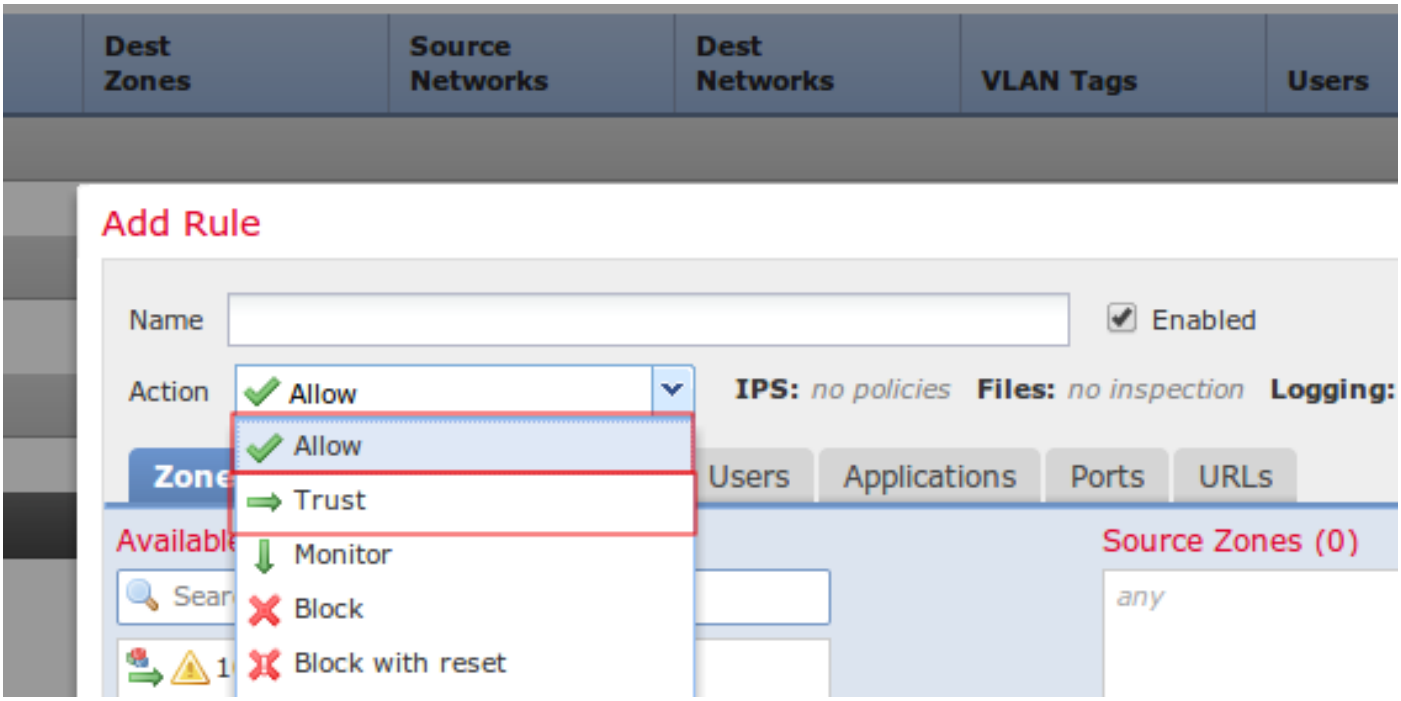

그림: 신뢰 규칙 컨피그레이션

3. 불필요한 규칙 사용 안 함

오래된 취약성과 패치가 적용된 취약성을 대상으로 하는 Snort 규칙을 비활성화할 수 있습니다. 성능을 개선하고 오탐을 줄입니다. FireSIGHT 권장 사항을 사용하면 이 작업을 지원할 수 있습니다. 또한 우선순위가 낮은 알림 또는 실행 가능하지 않은 알림을 자주 생성하는 규칙은 침입 정책에서 제거할 수 있는 좋은 후보가 될 수 있습니다.

4. 임계값

Threshold를 사용하여 침입 이벤트의 수를 줄일 수 있습니다. 이 옵션은 규칙이 일반 트래픽에서 제한된 수의 이벤트를 정기적으로 트리거할 것으로 예상되는 경우 구성하는 것이 좋지만, 특정 패킷 수 이상이 규칙과 일치하는 경우 문제를 나타낼 수 있습니다. 이 옵션을 사용하여 잡음 규칙에 의해 트리거되는 이벤트의 수를 줄일 수 있습니다.

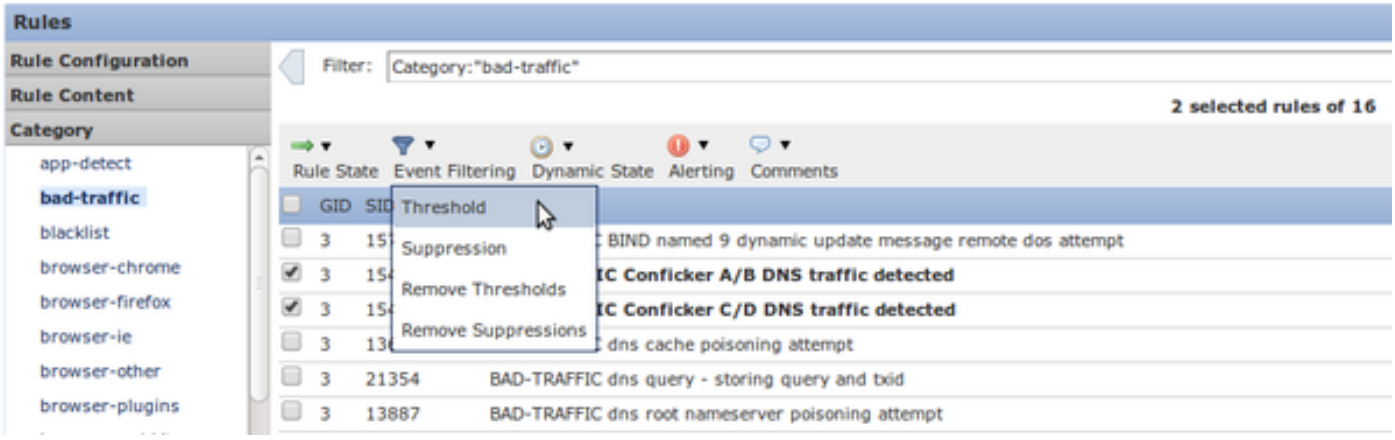

그림: 임계값 컨피그레이션

5. 삭제

Suppression을 사용하여 이벤트의 알림을 완전히 제거할 수 있습니다. Threshold(임계값) 옵션과 유사하게 구성됩니다.

> 주의: 이벤트가 생성되지 않더라도 Snort에서 트래픽을 처리해야 하므로 억제하면 성능 문제가 발생할 수 있습니다.

> 참고: 삭제 규칙을 삭제해도 트래픽이 삭제되지 않으므로, 삭제 규칙과 일치하는 경우 트래픽이 자동으로 삭제될 수 있습니다.

---

6. 빠른 경로 규칙

액세스 제어 정책의 Trust 및 Allow 규칙과 마찬가지로 Fast-Path 규칙도 검사를 우회할 수 있습니다. Cisco Technical Support는 일반적으로 빠른 경로(Fast-Path) 규칙을 사용하는 것을 권장하지 않습니다. 이러한 규칙은 디바이스 페이지의 고급 창에서 구성되며 액세스 제어 규칙은 거의 항상 충분한 반면 쉽게 간과될 수 있기 때문입니다.

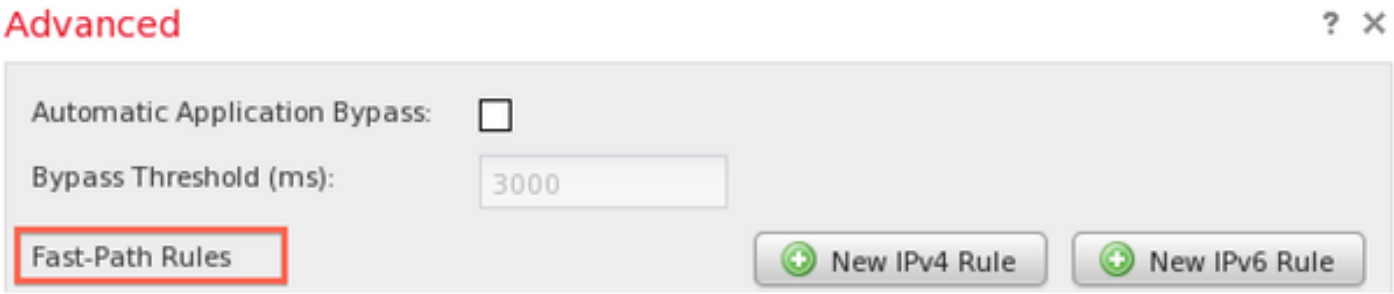

그림: 고급 창의 빠른 경로 규칙 옵션

빠른 경로 규칙을 사용할 때의 유일한 장점은 더 큰 최대 트래픽 볼륨을 처리할 수 있다는 것입니다. 빠른 경로 규칙은 하드웨어 레벨(NMSB라고 함)에서 트래픽을 처리하며 이론적으로 최대 200Gbps의 트래픽을 처리할 수 있습니다. 이와 달리 Trust 및 Allow 작업이 포함된 규칙은 NFE(Network Flow Engine)로 승격되며 최대 40Gbps의 트래픽을 처리할 수 있습니다.

> 참고: Fast-Path 규칙은 8000 Series 디바이스 및 3D9900에서만 사용할 수 있습니다.

---

7. 합격 규칙

특정 규칙이 특정 호스트의 트래픽에서 트리거되는 것을 방지하려면(해당 호스트의 다른 트래픽은 검사해야 함) pass type Snort 규칙을 사용합니다. 사실, 이것이 그것을 성취하기 위한 유일한 방법이다. 합격 규칙은 유효하지만 수동으로 작성되기 때문에 유지하기가 매우 어려울 수 있습니다. 또한 규칙 업데이트에 의해 패스 규칙의 원래 규칙이 수정되는 경우 관련된 모든 패스 규칙을 수동으로 업데이트해야 합니다. 그렇지 않으면 효과가 없을 수 있습니다.

8. SNORT_BPF 변수

침입 정책의 Snort_BPF 변수는 특정 트래픽이 검사를 우회하도록 합니다. 이 변수는 레거시 소프트웨어 버전의 첫 번째 선택 사항 중 하나였지만, Cisco Technical Support에서는 액세스 제어 정책 규칙을 사용하여 검사를 우회할 것을 권장합니다. 그 이유는 액세스 제어 정책 규칙이 더 세분화되고, 더 눈에 띄며, 구성이 훨씬 쉽기 때문입니다.

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.