침입 방지 성능 조정

다음 주제에서는 침입 방지 성능을 개선하는 방법을 설명합니다.

침입 방지 성능 조정 정보

Cisco는 시스템이 시도된 침입의 트래픽을 분석할 때 시스템의 성능을 향상시키는 여러 기능을 제공합니다. 다음 작업을 수행할 수 있습니다.

- 이벤트 대기열에서 허용할 패킷의 수를 지정할 수 있습니다. 또한, 스트림 리어셈블리 전후에, 대형 스트림으로 재구축되는 패킷에 대한 검사를 활성화 또는 비활성화할 수 있습니다.
- 침입 규칙에서 사용되는 PCRE에 대한 기본 일치 및 재귀 한도를 재정의하여 패킷 페이로드 콘텐츠를 검사할 수 있습니다.
- 여러 이벤트가 생성될 때 규칙 엔진이 패킷 또는 패킷 스트림당 둘 이상의 이벤트를 로깅하도록 하여 보고된 이벤트 이상의 정보를 수집할 수 있습니다.
- 패킷 및 규칙 레이턴시 임계값으로 보안과 디바이스 레이턴시 유지 필요성 사이의 균형을 적절한 수준으로 유지할 수 있습니다.
- 디바이스가 자체 성능을 모니터링하고 보고하는 방법에 대한 기본 매개변수를 구성할 수 있습니다. 이를 통해 시스템이 디바이스에서 성능 통계를 업데이트하는 간격을 지정할 수 있습니다.

사용자는 액세스 제어 정책을 기반으로 한 성능 설정을 구성하고, 해당 상위 액세스 제어 정책에 의해 호출된 모든 침입 정책에 적용합니다.

침입 방지 성능 조정 라이선스 요건

Threat Defense 라이선스

IPS

기본 라이선스

보호

침입 방지 성능 조정 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

침입에 대한 패턴 일치 제한

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다(**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Edit(**편집**)** > **More(**더보기**)** > **Advanced Settings(**고급 설정**)**).

새 UI의 패킷 플로우 라인 끝에 있는 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **2** **Performance Settings(**성능 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘(**View(**보기**)** (👁))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Performance Settings(**성능 설정**)** 팝업 창에서 **Pattern Matching Limits(**패턴 일치 제한**)**를 클릭합니다.

단계 **4** **Maximum Pattern States to Analyze Per Packet(**패킷당 분석할 최대 패턴 상태**)** 필드에 대기열에 넣을 이벤트의 최대 수 값을 입력합니다.

단계 **5** Snort 2에서 스트림 리어셈블리 전후에 대규모 데이터 스트림으로 재구축되는 패킷 검사를 비활성화하려면 **Disable Content Checks on Traffic Subject to Future Reassembly(**향후 리어셈블리 대상이 되는 트래픽에 대해 콘텐츠 확인 비활성화**)** 확인란을 선택합니다. 리어셈블리 전후의 검사에는 추가 프로세싱 오버헤드가 필요하므로 성능이 저하될 수 있습니다.

중요 Snort 3에서 **Disable Content Checks on Traffic Subject to the future Reassembly(**향후 리어셈블리할 트래픽에 대한 콘텐츠 검사 비활성화**)** 확인란 설정은 다음과 같습니다.

- Checked(선택됨) - 리어셈블리 전에 TCP 페이로드를 탐지함을 나타냅니다. 여기에는 스트림 리어셈블리 전후의 패킷 검사가 포함됩니다. 이 프로세스에는 더 많은 처리 오버헤드가 필요 하며 성능이 저하될 수 있습니다.
- Unchecked(선택하지 않음) - 리어셈블리 후 TCP 페이로드를 탐지함을 나타냅니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

침입 규칙용 정규식 제한 재정의

기본 정규 표현식 제한은 최소 수준의 성능을 보장합니다. 이러한 제한을 재정의하면 보안을 강화할 수 있지만, 비효율 정규식에 대한 패킷 평가를 허용함으로써 성능에 중대한 영향을 미칠 수 있습니다.

⚠

주의 손상 패턴의 영향에 대한 지식이 있는 숙련된 침입 규칙 작성가가 아닌 이상 기본 PCRE 제한값을 재정의하지 마십시오.

표 *1:* 정규식 제약 조건 옵션

옵션	설명
일치 제한 상태	**Match Limit(**일치 제한**)** 재정의 여부를 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Match Limit(**일치 제한**)**에 대해 구성된 값을 사용하려면 **Default(**기본값**)**를 선택합니다. • 무제한 시도를 허용하려면 **Unlimited(**무제한**)**를 선택합니다. • **Custom**을 선택하여 **Match Limit**의 제한값을 1 이상으로 지정하거나, 0으로 지정하여 PCRE 매치 평가를 완전히 비활성화합니다.
일치 제한	PCRE 정규식에 정의된 패턴에 일치시키려는 시도의 횟수를 지정합니다.
일치 반복 제한 상태	**Match Recursion Limit(**일치 반복 제한**)** 재정의 여부를 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Default**를 선택하여 **Match Recursion Limit**에 구성된 값을 사용합니다. • 무제한 반복을 허용하려면 **Unlimited(**무제한**)**를 선택합니다. • **Custom**을 선택하여 **Match Recursion Limit**의 제한값을 1 이상으로 지정하거나, 0으로 지정하여 PCRE 억제를 완전히 비활성화합니다. **Match Recursion Limit(**일치 반복 제한**)**가 작동하려면 반드시 **Match Limit(**일치 제한**)**보다 작아야 함을 참고하시기 바랍니다.
일치 반복 제한	패킷 페이로드에 대한 PCRE 정규식을 평가할 때 반복 수를 지정합니다.

관련 항목

개요: pcre 키워드

침입 규칙용 정규식 제한 재정의

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

새 UI의 패킷 플로우 라인 끝에 있는 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **2** **Performance Settings(**성능 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘(**View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Performance Settings(**성능 설정**)** 팝업 창에서 **Regular Expression Limits(**정규 표현식 제한**)**을 클릭합니다.

단계 **4** 침입 규칙용 정규식 제한 재정의, 3 페이지에서 설명한 모든 옵션을 수정할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

패킷 침입당 이벤트 생성 제한

침입 규칙 엔진은 규칙에 대한 트래픽을 평가할 때 주어진 패킷 또는 패킷 스트림에 대해 생성된 이벤트를 이벤트 대기열에 배치한 다음 대기열의 상위 이벤트를 사용자 인터페이스에 보고합니다. 침입 이벤트 로깅 제한을 구성할 때 대기열에 배치하고 로깅할 이벤트 수를 지정하고 대기열의 이벤트 순서를 결정할 기준을 선택할 수 있습니다.

표 *2:* 침입 이벤트 로깅 제한 옵션

옵션	설명
패킷당 저장된 최대 이벤트	주어진 패킷 또는 패킷 스트림에 대해 저장될 수 있는 최대 이벤트 수
패킷당 로깅된 최대 이벤트	주어진 패킷 또는 패킷 스트림에 대해 로깅될 수 있는 최대 이벤트 수. 이는 **Maximum Events Stored Per Packet(**패킷당 저장된 최대 이벤트**)** 값을 초과할 수 없습니다.
이벤트 로깅 우선 순위 지정 기준	이벤트 큐 내 이벤트 순서를 결정하는 데 사용되는 값. 최고 순위 이벤트는 사용자 인터페이스를 통해 보고됩니다. 사용자는 다음에서 선택할 수 있습니다. • `priority`. 이벤트 우선 순위에 따라 해당 큐에서 이벤트 순서를 결정하는 것. • `content_length`. 가장 긴 것으로 확인된 콘텐츠 일치에 따라 이벤트 순서를 결정하는 것. 이벤트가 콘텐츠 길이에 의해 순서가 정해질 때, 규칙 이벤트는 항상 디코더 및 전처리기 이벤트에 우선합니다.

패킷당 생성되는 침입 이벤트 제한

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

새 UI의 패킷 플로우 라인 끝에 있는 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **2** **Performance Settings(**성능 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘**(View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Performance Settings(**성능 설정**)** 팝업 창에서 **Intrusion Event Logging Limits(**침입 이벤트 로깅 제한**)** 탭을 클릭합니다.

단계 **4** 패킷 침입당 이벤트 생성 제한, 5 페이지의 모든 옵션을 수정할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

패킷 및 침입 규칙 레이턴시 임계값 구성

각 액세스 제어 정책은 지연 기반 설정으로 임계값을 사용해 패킷과 규칙 처리 성능을 관리합니다.

패킷 레이턴시 임계값은 처리 시간이 구성 가능한 임계값을 초과하는 경우 적용 가능한 디코더, 전처리기 및 규칙에 의해 패킷을 처리하는 데 드는 총 소요 시간을 측정합니다.

규칙 레이턴시 임계값은 각 규칙에서 개별 패킷을 처리하는 데 걸리는 시간을 측정하고, 처리 시간이 규칙 레이턴시 임계값(구성 가능한 연속 횟수)을 넘을 경우 위반 규칙 및 지정된 시간에 대한 관련 규칙 그룹을 동시에 중단하며, 일시 중단이 만료되면 해당 규칙을 복원합니다.

레이턴시 기반 성능 설정

기본적으로 시스템은 시스템에 구축된 최신 침입 규칙 업데이트에서 레이턴시 기반 성능 설정을 가져옵니다.

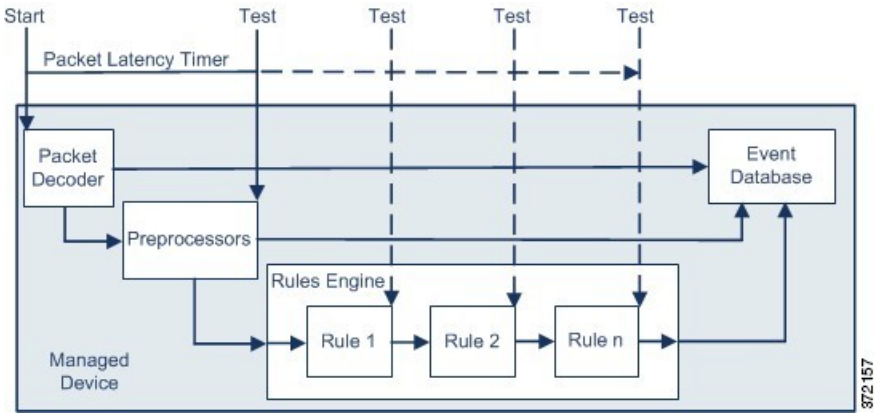
실제로 적용되는 레이턴시 설정은 액세스 제어 정책에 연결된 네트워크 분석 정책(NAP)의 보안 수준에 따라 달라집니다. 일반적으로 이것은 기본 NAP 정책입니다. 하지만 맞춤형 네트워크 분석 규칙이 구성되고 이러한 규칙 중에 기본 NAP 정책보다 더 안전한 NAP 정책을 지정하는 규칙이 있는 경우, 레이턴시 설정은 맞춤형 규칙 중 가장 안전한 NAP 규칙에 기반합니다. 기본 NAP 정책 또는 맞춤형 규칙이 맞춤형 NAP 정책을 호출하는 경우, 평가에 사용되는 보안 수준은 각 맞춤형 NAP 정책이 기반하는 시스템 제공 기본 정책입니다.

위 내용은 유효한 임계값 및 네트워크 분석 컨피그레이션이 상속되는지 또는 정책에서 직접 구성되는지 여부에 상관없이 적용됩니다.

패킷 레이턴시 임계값

패킷 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반 레이턴시 구현입니다.

레이턴시 임계값에서 파생된 레이턴시 이점과 성능의 반대 급부는 검사하지 않은 패킷에 공격이 포함될 수 있다는 점입니다. 디코더가 프로세스를 시작할 때 각 패킷의 타이머가 시작됩니다. 타이밍은 패킷의 모든 처리가 종료되거나, 처리 시간이 타이밍 테스트 지점의 임계값을 초과할 때까지 계속됩니다.



위 그림에 표시된 것처럼, 패킷 레이턴시 타이밍은 다음과 같은 테스트 지점에서 테스트됩니다.

- 모든 디코더 및 전처리기의 처리가 완료된 이후 및 규칙 처리가 시작되기 이전
- 각 규칙에 따라 처리된 이후

처리 시간이 테스트 지점의 임계값을 초과할 경우, 패킷 검사가 중단됩니다.

팁 루틴 TCP 스트림 또는 IP 조각 리어셈블리 시간은 총 패킷 처리 시간에 포함되지 않습니다.

패킷 레이턴시 임계값은 디코더, 전처리기 또는 패킷 처리 규칙에 의해 시작된 이벤트에 대해서는 영향을 미치지 않습니다. 적용 가능한 디코더, 전처리기 또는 규칙은 보통 패킷이 완전히 처리될 때까지, 또는 레이턴시 임계값이 초과하여 패킷 처리가 끝날 때까지, 어느 쪽이든 먼저 될 때까지 작동합

니다. 삭제 규칙이 인라인 배포에서 침입을 탐지하는 경우, 삭제 규칙은 이벤트를 시작하며 패킷은 삭제됩니다.

참고 패킷 레이턴시 임계값 위반으로 인해 해당 패킷 처리가 끝난 후 규칙에 반하여 평가되는 패킷은 없습니다. 이벤트를 시작했을 수도 있는 규칙은 해당 이벤트를 시작할 수 없으며, 삭제 규칙을 위해 패킷을 삭제할 수 없습니다.

패킷 레이턴시 임계값을 사용하면 과도한 처리 시간이 요구되는 패킷 검사를 중단함으로써 패시브 및 인라인 구축 시 시스템 성능을 향상하고, 인라인 구축 시 레이턴시를 줄일 수 있습니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 패시브 및 인라인 배포에서 과도한 시간을 들여 여러 규칙별 패킷 검사를 순차적으로 수행하는 경우
- 인라인 배포에서 네트워크 성능이 저하된 경우(예: 누군가 대용량 파일을 다운로드하여 패킷 처리 속도가 느려짐)

수동 배포에서 패킷의 처리를 중지하면 처리는 다음 패킷으로 간단하게 옮겨가므로 네트워크 성능 복구에 도움이 되지 않을 수도 있습니다.

패킷 레이턴시 임계값 참고 사항

기본적으로 패킷 처리에 대한 레이턴시 기반 성능 설정은 비활성화됩니다. 원한다면 활성화할 수도 있습니다. 그러나 Cisco에서는 임계값 설정 기본값 변경을 권장하지 않습니다.

아래 항목의 정보는 맞춤형 값을 지정하도록 선택하는 경우에만 적용됩니다.

표 ***3:*** 패킷 레이턴시 임계값 옵션

옵션	설명
임계값(마이크로초)	패킷의 검사가 중지될 때, 마이크로초로 시간을 지정합니다.

패킷 레이턴시 임계값 활성화

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

새 UI의 패킷 플로우 라인 끝에 있는 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **2** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘(**View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 팝업 창에서 **Packet Handling(**패킷 처리**)**을 클릭합니다.

단계 **4** **Enable(**활성화**)** 확인란을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

패킷 레이턴시 임계값 구성

기본적으로 패킷 처리에 대한 레이턴시 기반 성능 설정은 비활성화됩니다. 원한다면 활성화할 수도 있습니다. 그러나 Cisco에서는 임계값 설정 기본값 변경을 권장하지 않습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

새 UI의 패킷 플로우 라인 끝에 있는 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **2** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

시스템 ( ) > **Monitoring(**모니터링**)** > **Statistics(**통계**)**

단계 **3** 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **4** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 팝업 창에서 **Packet Handling(**패킷 처리**)**을 클릭합니다.

기본적으로는 **Installed Rule Update(**설치된 규칙 업데이트**)**가 선택됩니다. 이 기본값을 사용하는 것이 좋습니다.

표시되는 값은 자동화된 설정을 반영하지 않습니다.

단계 **5** 맞춤형 값을 지정하려면

- **Enabled(**활성화**)** 확인란을 선택하고, 패킷 레이턴시 임계값 참고 사항, 8 페이지에서 권장 최소 **Threshold(**임계값**)** 설정을 확인합니다.
- 패킷 처리 탭과 규칙 처리 탭 둘 다에서 사용자 지정 값을 지정해야 합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

규칙 레이턴시 임계값

규칙 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반 레이턴시 구현입니다.

레이턴시 임계값에서 파생된 레이턴시 이점과 성능의 반대 급부는 검사하지 않은 패킷에 공격이 포함될 수 있다는 점입니다. 타이머는 패킷이 규칙 그룹에 대해 처리될 때마다 처리 시간을 측정합니다. 규칙 처리 시간이 지정된 규칙 레이턴시 임계값을 초과하는 모든 경우, 시스템은 계수기를 증대합니다. 후속 임계값 위반 수가 지정된 수에 도달하는 경우, 시스템은 다음 작업을 수행합니다.

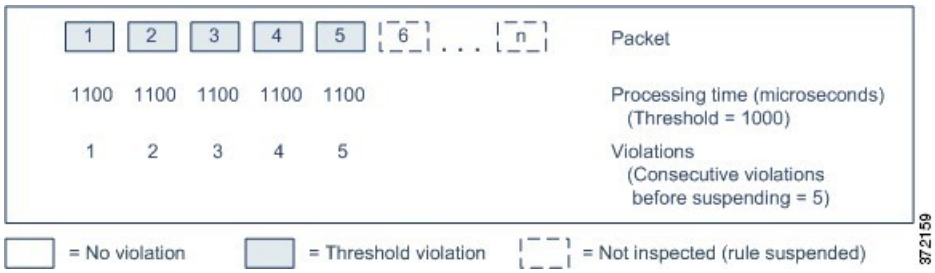
- 지정된 기간 동안 규칙을 중지합니다.
- 규칙이 중지되었음을 나타내는 이벤트를 시작합니다.
- 중지가 만료되면 규칙을 재활성화합니다.
- 규칙이 재활성화되었음을 나타내는 이벤트를 시작합니다.

그룹 규칙이 중지되거나 규칙 위반이 연속적이지 않은 경우 시스템은 계수기를 0에 맞춥니다. 규칙을 중지하기 전에 여러 개의 연속되는 위반을 허용하면 사용자는 가끔 일어나는 규칙 위반, 즉 성능에 미치는 영향이 무시할 만한 수준인 위반을 무시해버리고 사용자는 규칙 레이턴시 임계값을 반복적으로 초과하는 규칙에 미치는 더욱 중대한 영향력에 집중하게 됩니다.

다음의 예시는 규칙 중단으로 귀결되지 않는 다섯 가지의 연속 규칙 처리 시간을 보여줍니다.

위 예시에서, 처음 3개 패킷의 각각을 처리하는 데 필요한 시간은 1000마이크로초의 규칙 레이턴시 임계값을 위반하며, 각 위반과 함께 위반 계수기도 증대됩니다. 네 번째 패킷 처리는 임계값을 위반하지 않으며, 위반 계수기는 0으로 재설정됩니다. 다섯 번째 패킷은 임계값을 위반하며, 위반 계수기는 1에서 다시 시작합니다.

다음의 예시는 규칙 중단으로 귀결되는 다섯 가지의 연속 규칙 처리 시간을 보여줍니다.



두 번째 예에서, 다섯 개의 패킷 중 각각을 처리하는 데 필요한 시간은 1000마이크로초의 규칙 레이턴시 임계값을 위반합니다. 규칙 그룹은 각 패킷에 대한 1100마이크로초의 규칙 처리 시간이 명시된 5회 연속 위반 기간 동안 1000마이크로초의 임계값을 초과하므로 중지됩니다. 패킷 6 또는 그보다 큰 수(n)로 표시된 모든 후속 패킷은 중지가 만료될 때까지 중지된 규칙에 반해 검토되지 않습니다. 규칙이 재활성화된 후에 추가 패킷이 발생하는 경우, 위반 계수기는 0에서 다시 시작됩니다.

규칙 레이턴시 임계값은 패킷을 처리하는 규칙에 의해 시작된 침입 이벤트에는 어떤 영향도 미치지 않습니다. 규칙은 규칙 처리 시간이 임계값을 초과하는지 여부에 상관없이 패킷에서 탐지된 모든 침입에 대한 이벤트를 시작합니다. 침입을 탐지하는 규칙이 인라인 배포에서 삭제 규칙인 경우, 패킷은 삭제됩니다. 삭제 규칙이 패킷에서 규칙 중단으로 귀결되는 침입을 탐지하는 경우, 삭제 규칙은 침입 이벤트를 시작하고, 패킷은 삭제되며, 해당 규칙 및 모든 관련 규칙은 중지됩니다.

참고 패킷은 중단된 규칙에 반해 평가되지 않습니다. 이벤트를 시작했을 수도 있는 중지된 규칙은 해당 이벤트를 시작할 수 없으며, 삭제 규칙을 위해 패킷을 삭제할 수 없습니다.

규칙 레이턴시 임계값을 사용하면 대부분의 패킷 처리 시간을 관장하는 규칙을 중지함으로써 수동 배포 및 인라인 배포에 있어 시스템 성능을 향상하고, 인라인 배포 시 레이턴시를 줄일 수 있습니다. 패킷은 과부하된 디바이스에 복원할 수 있는 시간을 제공하면서 구성 가능한 시간이 만료될 때까지 중지된 규칙에 반해 다시 평가되지 않습니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 급히 쓰여진, 대개 테스트되지 않는 규칙에 과도한 양의 처리 시간이 필요한 경우
- 네트워크 성능이 저하된 경우(예: 누군가 대용량 파일을 다운로드하여 패킷 검사 속도가 느려짐)

규칙 레이턴시 임계값 참고

기본적으로 패킷 및 규칙 처리에 모두 사용되는 레이턴시 기반 성능 설정은 가장 최근에 배포된 침입 규칙 업데이트를 통해 자동으로 입력되며, 기본값을 변경하지 않는 것이 좋습니다.

이 항목의 정보는 사용자 지정 값을 지정하도록 선택하는 경우에만 적용됩니다.

규칙 레이턴시 임계값은 시간 규칙이 **Consecutive Threshold Violations Before Suspending Rule(**규칙 중지 전 연속 임계값 위반**)**에 지정된 연속된 횟수 동안 **Threshold(**임계값**)**를 초과하는 패킷을 처리하기 시작할 때 **Suspension Time(**중지 시간**)**에 지정된 시간 동안 규칙을 중지합니다.

규칙이 중지되었을 때 규칙 134:1을 활성화하여 이벤트를 생성할 수 있고, 중지된 규칙이 활성화되었을 때는 규칙 134:2를 활성화하여 이벤트를 생성할 수 있습니다. 침입 규칙 상태 옵션의 내용을 참조하십시오.

표 *4:* 규칙 레이턴시 임계값 옵션

옵션	설명
임계값	패킷을 검토할 때 규칙이 초과해서는 안 되는 시간을 마이크로초로 지정합니다.
규칙 중지 전 연속 임계값 위반	**Threshold**에 대해 지정된 시간보다 오래 소요될 수 있는 연속 시간 횟수를 지정하여 규칙이 중단되기 전에 패킷을 검사할 수 있도록 합니다.
중단 시간	규칙 그룹을 중지하려면 초 단위 시간을 지정합니다.

규칙 레이턴시 임계값 구성

기본적으로 패킷 및 규칙 처리에 모두 사용되는 레이턴시 기반 성능 설정은 가장 최근에 배포된 침입 규칙 업데이트를 통해 자동으로 입력되며, 기본값을 변경하지 않는 것이 좋습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭합니다.

새 UI의 패킷 플로우 라인 끝에 있는 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **2** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘**(View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Latency-Based Performance Settings(**레이턴시 기반 성능 설정**)** 팝업 윈도우에서 **Rule Handling(**규칙 처리**)**를 선택합니다.

기본적으로는 **Installed Rule Update(**설치된 규칙 업데이트**)**가 선택됩니다. 이 기본값을 사용하는 것이 좋습니다.

표시되는 값은 자동화된 설정을 반영하지 않습니다.

단계 **4** 선택하면 맞춤형 값을 지정할 수 있습니다.

- 규칙 레이턴시 임계값 참고, 11 페이지에 있는 모든 옵션을 설정할 수 있습니다.
- 패킷 처리 탭과 규칙 처리 탭 둘 다에서 사용자 지정 값을 지정해야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 이벤트를 생성하고 싶다면 레이턴시 규칙 134:1 및 134:2를 활성화합니다. 자세한 내용은 침입 규칙 상태 옵션를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

침입 성능 통계 로깅 구성

시간(초) 샘플링 및 패킷 수 최소화

성능 통계량 업데이트 사이에 지정된 시간(초)이 소요된 경우, 시스템은 패킷의 지정된 수를 분석했는지 확인합니다. 확인된 경우, 시스템은 성능 통계량을 업데이트합니다. 그렇지 않은 경우, 시스템은 패킷의 지정된 수를 분석할 때까지 기다립니다.

주의 Sample time(샘플 시간)을 매우 낮은 값(예: 1초)으로 구성하면 디바이스에 큰 영향을 줄 수 있습니다. 디바이스에 로깅된 성능 통계는 디스크 공간 문제를 야기하고 디바이스의 작동에 영향을 줄 수 있습니다. 따라서 너무 낮은 값을 구성하지 않는 것이 좋습니다.

문제 해결 옵션: 로그 세션/프로토콜 배포

지원팀은 문제 해결 통화 중 사용자에게 프로토콜 배포, 패킷 길이 및 포트 통계량을 로깅할 것을 요청할 수 있습니다.

주의 지원팀이 지시할 때만 **Log Session/Protocol Distribution(**로그 세션/프로토콜 배포**)**을 활성화하십시오.

문제 해결 옵션: 요약

문제 해결 통화 중에 지원팀에서 Snort® 프로세스가 종료되거나 다시 시작된 경우에만 성능 통계를 계산하도록 시스템을 구성하라고 요청할 수 있습니다. 이 옵션을 활성화하려면, 또한 반드시 **Log Session/Protocol Distribution(**로그 세션/프로토콜 배포**)** 옵션을 선택합니다.

주의 지원팀이 지시할 때만 **Summary(**요약**)**를 활성화하십시오.

침입 성능 통계 로깅 구성

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭한 다음 **Performance Settings(**성능 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

새 UI의 패킷 플로우 라인 끝에 있는 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

보기 아이콘**(View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 표시되는 팝업 윈도우에서 **Performance Statistics(**성능 통계**)**를 클릭합니다.

단계 **3** 침입 성능 통계 로깅 구성, 13 페이지에 설명된 대로 **Sample time(**샘플 시간**)** 또는 **Minimum number of packets(**패킷 최소 수**)**를 수정합니다.

주의 **Sample time(**샘플 시간**)**을 매우 낮은 값(예: 1초)으로 구성하면 디바이스에 큰 영향을 줄 수 있습니다. 디바이스에 로깅된 성능 통계는 디스크 공간 문제를 야기하고 디바이스의 작동에 영향을 줄 수 있습니다. 따라서 너무 낮은 값을 구성하지 않는 것이 좋습니다.

단계 **4** 지원팀의 요청이 있는 경우에만 선택적으로, **Troubleshoot Options(**문제 해결 옵션**)** 섹션을 확장하고 해당 옵션을 수정합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.