특정 위협 탐지

다음 주제에서는 네트워크 분석 정책에서 전처리기를 사용해 특정 위협을 탐지하는 방법을 설명합니다.

- 특정 위협 탐지 소개, 1 페이지
- 특정 위협 탐지 라이선스 요건, 1 페이지
- 특정 위협 탐지 요구 사항 및 사전 요건, 2 페이지
- Back Orifice 탐지, 2 페이지
- 포트스캔 탐지, 4 페이지
- 속도 기반 공격 방지, 12 페이지

특정 위협 탐지 소개

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

네트워크 분석 정책에서 여러 전처리기를 사용하여 Back Orifice 공격, 여러 포트스캔 유형, 그리고 과도한 트래픽으로 네트워크를 무력화하려는 속도 기반 공격과 같은 사용자의 모니터링된 네트워크에 대한 특정 위협을 탐지할 수 있습니다. 전처리기에 특정한 GID 서명이 활성화되면 웹의 네트워크 분석 정책이 비활성화된 것으로 표시됩니다. 그러나 전처리기는 사용 가능한 기본 설정을 사용하여 디바이스에서 켜집니다.

보안 없이 전송되는 민감한 수치 데이터를 탐지하려면 침입 정책에서 구성하는 민감한 데이터 탐지 기능을 사용할 수도 있습니다.

특정 위협 탐지 라이선스 요건

FTD 라이선스

위협

기본 라이선스

보호

특정 위협 탐지 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

Back Orifice 탐지

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

Firepower System은 Back Orifice 프로그램의 존재를 탐지하는 전처리기를 제공합니다. 이 프로그램은 Windows 호스트에 대한 관리자 액세스 권한을 얻는 데 사용할 수 있습니다.

Back Orifice 탐지 전처리기

Back Orifice 전처리기는 Back Orifice 매직 쿠키인 "*!*QWTY?"(패킷의 처음 8바이트에 있으며 XOR로 암호화됨)에 대한 UDP 트래픽을 분석합니다.

Back Orifice 프리프로세서는 구성 페이지가 있지만, 구성 옵션은 없습니다. 활성화한 경우, 전처리기가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하게 하려면 전처리기 규칙을 활성화해야 합니다.

표 *1: Back Orifice GID:SID*

전처리기 규칙 **GID:SID**	설명
105:1	Back Orifice 트래픽이 탐지됨
105:2	Back Orifice 클라이언트 트래픽이 탐지됨

전처리기 규칙 **GID:SID**	설명
105:3	Back Orifice 서버 트래픽이 탐지됨
105:4	Back Orifice Snort 버퍼 공격이 탐지됨

Back Orifice 탐지

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 **3** 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **5** **Specific Threat Detection(**특정 위협 탐지**)**의 **Back Orifice Detection(Back Orifice** 탐지**)**가 비활성화되었다면 **Enabled**를 클릭합니다.

참고 Back Orifice에는 사용자가 설정하는 옵션이 없습니다.

단계 **6** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 Back Orifice Detection(Back Orifice 탐지) 규칙 105:1, 105:2, 105:3 또는 105:4를 활성화합니다. 자세한 내용은 침입 규칙 상태 및 Back Orifice 탐지 전처리기, 2 페이지의 내용을 참조하십시오.
- Deploy configuration changes(구성 변경 사항 구축), Firepower Management Center 관리 가이드 참조.

포트스캔 탐지

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

포트스캔은 공격에 앞서 공격자가 종종 사용하는 네트워크 정찰의 형태입니다. 포트스캔에서 공격자는 특별히 고안된 패킷을 대상 호스트로 전송합니다. 호스트가 응답하는 패킷을 검사하여 공격자는 종종 호스트에서 어떤 포트가 열려 있는지, 그리고 직접적으로 또는 추론에 의해 이러한 포트에서 어떤 애플리케이션 프로토콜이 실행 중인지 확인할 수 있습니다.

포트스캔 자체는 공격의 증거가 되지 못합니다. 실제로, 공격자가 사용하는 포트스캔 기법 중 일부는 네트워크의 합법적인 사용자들도 사용할 수 있습니다. Cisco의 포트스캔 탐지기는 활동의 패턴을 탐지하여 어떤 포트스캔이 악의적일 수 있는지를 확인하도록 설계되었습니다.

주의 내부 리소스에서의 디바이스 부하 균형 검사. 포트스캔 탐지가 예상대로 작동하지 않는 경우, 민감도 레벨을 **High(**높음**)**로 구성해야 할 수 있습니다.

Snort 3으로 업그레이드하고 버전 7.2.0에 도입된 포트스캔 기능을 사용하는 것이 좋습니다. 자세한 내용은 Firepower Management Center Snort 3 구성 가이드 및 Snort 3 검사기 참조의 내용을 참조하십시오.

포트스캔 유형, 프로토콜 및 필터링된 민감도 레벨

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

공격자들은 네트워크에 대한 프로브를 위해 여러 방법을 사용할 것입니다. 이들은 종종, 하나의 프로토콜 유형이 차단되면 다른 것을 사용할 수 있도록 대상 호스트에서 서로 다른 응답을 이끌어내기 위해 여러 프로토콜을 사용합니다.

표 *2:* 프로토콜 유형

프로토콜	설명
TCP	SYN 스캔, ACK 스캔, TCP connect() 스캔, 그리고 Xmas tree, FIN, NULL 등 특이한 플래그 조합의 스캔과 같은 TCP 프로브를 탐지합니다.
UDP	제로바이트 UDP 패킷과 같은 UDP 프로브를 탐지합니다.
ICMP	ICMP 에코 요청(ping)을 탐지합니다.
IP	IP 프로토콜 스캔을 탐지합니다. 이 스캔은 TCP 및 UDP 스캔과 다릅니다. 공격자가 열린 포트를 찾는 대신 대상 호스트에서 어떤 IP 프로토콜이 지원되는지를 알아보려고 하기 때문입니다.

포트스캔은 일반적으로 대상 호스트의 수, 스캔하는 호스트의 수, 스캔되는 포트의 수를 기반으로 네 가지 유형으로 구분됩니다.

표 *3:* 포트스캔 유형

유형	설명
포트스캔 탐지	공격자가 단일 대상 호스트에서 여러 포트를 스캔하기 위해 하나 또는 소수의 호스트를 사용하는 일대일 포트스캔입니다. 일대일 포트스캔의 특성: • 스캔하는 호스트 수가 적음 • 단일 호스트가 스캔됨 • 스캔되는 포트 수가 많음 이 옵션은 TCP, UDP 및 IP 포트스캔을 탐지합니다.
포트 스윕	공격자가 하나 또는 여러 호스트를 사용하여 여러 대상 호스트에서 단일 포트를 스캔하는 일대다 포트 스윕입니다. 포트 스윕에는 다음과 같은 특징이 있습니다. • 스캔하는 호스트 수가 적음 • 스캔되는 호스트 수가 많음 • 스캔되는 고유한 포트 수가 적음 이 옵션은 TCP, UDP, ICMP 및 IP 포트 스윕을 탐지합니다.

유형	설명
Decoy 포트스캔	공격자가 실제 스캐닝 IP 주소와 스푸핑된 소스 IP 주소를 혼합하는 일대일 포트스캔입니다. Decoy 포트스캔에는 다음과 같은 특징이 있습니다. • 많은 수의 스캐닝 호스트 • 한 번만 스캐닝된 적은 수의 포트 • 스캐닝된 단일 (또는 적은 수의) 호스트 Decoy 포트스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.
분산형 포트스캔	여러 호스트가 개방형 포트를 위해 단일 호스트를 쿼리하는 다대일 포트스캔입니다. 분산형 포트스캔에는 다음과 같은 특징이 있습니다. • 많은 수의 스캐닝 호스트 • 한 번만 스캐닝된 많은 수의 포트 • 스캐닝된 단일 (또는 적은 수의) 호스트 분산형 포트스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.

포트스캔 탐지기가 프로브에 대해 알게 되는 정보는 대개 검토된 호스트에서 음수 응답이 표시되는 것을 기반으로 합니다. 예를 들어, 웹 클라이언트가 웹 서버에 연결을 시도할 때, 클라이언트는 포트 80/tcp를 사용하며 서버는 해당 포트가 열려 있도록 하는 역할을 수행할 수 있습니다. 하지만 서버를 검토할 때, 공격자는 서버의 웹 서비스 제공 여부를 미리 확인할 수 없습니다. 포트스캔 탐지기에 음수 응답(즉 ICMP에 연결할 수 없는 패킷 또는 TCP RST 패킷)이 표시되면 해당 응답을 잠재적 포트스캔으로 기록합니다. 이러한 프로세스는 대상 호스트가 음수 응답을 필터링하는 방화벽 또는 라우터와 같은 디바이스의 다른 편에 있는 경우 더욱 복잡합니다. 이 경우 포트스캔은 사용자가 선택한 민감도 레벨을 기반으로 필터링된 포트스캔 이벤트를 생성할 수 있습니다.

표 ***4:*** 민감도 레벨

레벨	설명
낮음	대상 호스트에서 부정적인 응답만 탐지합니다. 이 민감도 레벨을 선택하면 오탐을 억제할 수 있지만, 일부 포트스캔 유형(느린 스캔, 필터링된 스캔)을 놓칠 수 있습니다. 이 레벨은 포트스캔 탐지에 가장 짧은 시간 창을 사용합니다.

레벨	설명
중간	호스트에 대한 연결 수를 기반으로 포트스캔을 탐지합니다. 즉, 필터링된 포트스캔을 탐지할 수 있습니다. 그러나 네트워크 주소 변환기와 프록시 등 매우 활동적인 호스트는 오탐을 생성할 수 있습니다. 이 유형의 오탐을 완화하려면 이러한 활동적인 호스트의 IP 주소를 **Ignore Scanned(**스캔을 탐지하지 않음**)** 필드에 추가할 수 있습니다. 이 레벨은 포트스캔 탐지에 좀 더 긴 시간 창을 사용합니다.
높음	시간 창을 기반으로 포트스캔을 탐지합니다. 즉, 시간 기반 포트스캔을 탐지할 수 있습니다. 그러나 이 옵션을 사용할 경우 **Ignore Scanned(**스캔을 탐지하지 않음**)** 및 **Ignore Scanner(**스캐너를 탐지하지 않음**)** 필드에 IP 주소를 지정하여 시간에 따라 탐지기를 신중하게 조정해야 합니다. 이 레벨은 포트스캔 탐지에 훨씬 긴 시간 창을 사용합니다.

포트스캔 이벤트 생성

포트스캔 탐지가 활성화되면, 생성기 ID(GID) 122 및 SID 1에서 27 사이의 Snort ID(SID)(으)로 규칙을 활성화해야 다양한 포트스캔과 포트 스윕을 탐지할 수 있습니다.

참고 포트스캔 연결 탐지기에서 생성된 이벤트의 경우, 프로토콜 번호는 255로 설정됩니다. 포트스캔은 기본적으로 연결할 특정 프로토콜이 없기 때문에, IANA(Internet Assigned Numbers Authority, 인터넷 할당 번호 관리기관)에는 그에 할당된 프로토콜 번호가 없습니다. IANA는 255를 예약된 번호로 지정하여 해당 번호가 포트스캔 이벤트에서 사용되는 경우 해당 이벤트에 대해 연결된 프로토콜이 없음을 나타냅니다.

표 *5:* 포트스캔 탐지 ***SID(GID 122)***

포트스캔 유형	프로토콜	민감도 수준	전처리기 규칙 **SID**
포트스캔 탐지	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	1 5 17 21 이벤트를 생성하지 않습니다. 이벤트를 생성하지 않습니다. 9 13
포트 스윕	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	3, 27 7 19 23 25 26 11 15
Decoy 포트스캔	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	2 6 18 22 이벤트를 생성하지 않습니다. 이벤트를 생성하지 않습니다. 10 14

포트스캔 유형	프로토콜	민감도 수준	전처리기 규칙 **SID**
분산형 포트스캔	TCP UDP ICMP IP	낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음 낮음 중간 또는 높음	4 8 20 24 이벤트를 생성하지 않습니다. 이벤트를 생성하지 않습니다. 12 16

포트스캔 이벤트 패킷 보기

관련 전처리기 규칙을 활성화하면, 포트스캔 탐지기는 다른 모든 침입 이벤트를 수행할 때 표시될 수 있는 침입 이벤트를 생성합니다. 그러나, 패킷 보기에 표시되는 정보는 다른 유형의 침입 이벤트와는 다릅니다.

포트스캔 이벤트에 대한 패킷 보기로 드릴 다운하는 침입 이벤트 보기를 사용하는 것으로 시작합니다. 단일 포트스캔 이벤트가 여러 패킷에 기반하므로 포트스캔 패킷을 다운로드할 수 없습니다. 그러나, 포트스캔 패킷 보기는 모든 가용 패킷 정보를 제공합니다.

어떤 IP 주소에서도 주소를 클릭하여 콘텍스트 메뉴를 확인하고, **whois**를 선택하여 IP 주소 조회를 수행하거나 **View Host Profile(**호스트 프로파일 보기**)**을 선택하여 해당 호스트의 호스트 프로파일을 확인할 수 있습니다.

표 ***6:*** 포트스캔 패킷 보기

정보	설명
디바이스	이벤트를 탐지한 디바이스입니다.
시간	이벤트가 발생한 시간입니다.
메시지	전처리기에서 생성된 이벤트 메시지입니다.
Source IP(소스 IP)	스캐닝하는 호스트의 IP 주소입니다.
Destination IP(대상 IP)	스캐닝된 호스트의 IP 주소입니다.
우선 순위 집계	스캐닝된 호스트로부터의 음수 응답 수(예를 들어, TCP RSTs 및 ICMP에 도달할 수 없는)입니다. 음수 응답 수가 많을수록 우선 순위가 높습니다.
연결 집계	호스트에 연결된 활성 연결 수입니다. 이 값은 TCP 및 IP와 같은 연결 기반 스캔의 경우 더 정확합니다.

정보	설명
IP 집계	스캐닝된 호스트에 연결된 IP 주소가 변경된 횟수입니다. 예를 들어, 첫 번째 IP 주소가 10.1.1.1인 경우, 두 번째 IP는 10.1.1.2이며, 3번째 IP는 10.1.1.1이며, 다음으로 IP 수는 3입니다. 이 번호는 프록시 및 DNS 서버 등 활성 호스트의 경우 덜 정확합니다.
스캐너/스캐닝된 IP 범위	스캔 유형에 따른 스캐닝된 호스트 또는 스캐닝하는 호스트의 IP 주소 범위입니다. 포트 스윕의 경우, 이 필드는 스캐닝된 호스트의 IP 범위를 보여줍니다. 포트스캔의 경우, 이는 스캐닝하는 호스트의 IP 범위를 보여줍니다.
포트/프로토콜 집계	TCP와 UDP 포트스캔의 경우, 스캐닝되고 있는 포트가 변경된 횟수입니다. 예를 들어, 스캐닝된 첫 번째 포트가 80인 경우, 스캐닝된 두 번째 포트는 8080이고, 스캐닝된 세 번째 포트는 다시 80이며, 다음 포트 수는 3입니다. IP 프로토콜 포트스캔의 경우, 스캐닝된 호스트에 연결하기 위해 사용되고 있는 프로토콜의 변경 횟수입니다.
포트/프로토콜 범위	TCP와 UDP 포트스캔의 경우, 스캐닝된 포트 범위입니다. IP 프로토콜 포트스캔의 경우, 스캐닝된 호스트에 연결하려고 시도하는 데 사용되는 IP 프로토콜 수의 범위입니다.
개방 포트	스캐닝된 호스트에 개방된 TCP 포트입니다. 이 필드는 포트스캔이 하나 이상의 개방형 포트를 탐지하는 경우에만 나타납니다.

포트스캔 탐지 구성

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

포트스캔 탐지 구성 옵션을 사용하면 포트스캔 탐지기가 스캔 활동을 보고하는 방식을 세부적으로 조정할 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 **3** 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 설정을 클릭합니다.

단계 **5** **Specific Threat Detection(**특정 위협 탐지**)**의 **Portscan Detection(**포트스캔 탐지**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **Portscan Detection(**포트스캔 탐지**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** **Protocol(**프로토콜**)** 필드에 활성화할 프로토콜을 지정합니다.

참고 TCP를 통해 스캔을 탐지할 수 있도록 TCP 스트림 프로세싱이 활성화되었는지, 그리고 UDP를 통해 스캔을 탐지할 수 있도록 UDP 스트림 프로세싱이 활성화되었는지 확인해야 합니다.

단계 **8** **Scan Type(**스캔 유형**)** 필드에 탐지할 포트스캔 유형을 지정합니다.

단계 **9** **Sensitivity Level(**민감도 수준**)** 목록에서 수준을 선택합니다(포트스캔 유형, 프로토콜 및 필터링된 민감도 레벨, 4 페이지 참조).

단계 **10** 포트스캔 활동의 징후에 대한 특정 호스트를 모니터링하려면, **Watch IP(IP** 감시**)** 필드에 호스트 IP 주소를 입력합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 모든 네트워크 트래픽을 감시하려면 필드에 아무것도 입력하지 마십시오.

단계 **11** 호스트를 스캐너로 간주해 무시하려면, **Ignore Scanners(**스캐너 무시**)** 필드에 호스트 IP 주소를 입력합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다.

단계 **12** 호스트를 스캔 대상으로 간주해 무시하려면, **Ignore Scanned(**스캔한 대상 무시**)** 필드에 호스트 IP 주소를 입력합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다.

팁 **Ignore Scanners(**스캐너 무시**)**와 **Ignore Scanned(**스캔한 대상 무시**)** 필드를 이용해 네트워크에서 특별히 활성화한 호스트를 표시합니다. 시간이 지남에 따라 호스트 목록을 변경해야 합니다.

단계 **13** 중앙 스트림에서 선택된 세션의 모니터링을 중지하려면, **Detect Ack Scans(Ack** 스캔 탐지**)** 확인란을 선택 취소합니다.

참고 중앙 스트림 세션의 탐지는 ACK 스캔을 확인하는 데 도움이 되지만 특히 트래픽 과부하로 패킷을 삭제한 네트워크에 잘못된 이벤트를 발생시킬 수 있습니다.

단계 **14** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 포트스캔 탐지가 다양한 포트스캔과 포트 스윕을 탐지하게 하려면, 규칙 122:1~122:27을 활성화합니다. 자세한 내용은 침입 규칙 상태 및 포트스캔 이벤트 생성, 7 페이지의 내용을 참조하십시오.
- Deploy configuration changes(구성 변경 사항 구축), Firepower Management Center 관리 가이드 참조.

속도 기반 공격 방지

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

속도 기반 공격은 공격을 저지르는 연결 또는 반복된 시도의 빈도에 따른 공격입니다. 속도 기반 탐지 기준을 사용하여 속도 기반 공격이 발생할 때 이를 탐지하고 공격이 발생하는 경우 이에 반응한 후 공격이 중단되면 일반 탐지 설정으로 돌아갈 수 있습니다.

네트워크의 호스트로 향하는 과도한 활동을 탐지하는 속도 기반 필터를 포함하도록 네트워크 분석 정책을 구성할 수 있습니다. 인라인 모드로 구축된 매니지드 디바이스에서 이 기능을 사용하여 지정된 시간 동안 속도 기반 공격을 차단한 후 이벤트만 생성되고 트래픽은 삭제하지 않는 상태로 되돌릴 수 있습니다.

SYN 공격 방지 옵션을 통해 SYN 플러드 공격에 대해 네트워크 호스트를 보호할 수 있습니다. 일정 기간 동안 발견된 패킷 수에 따라 개별 호스트 또는 전체 네트워크를 보호할 수 있습니다. 디바이스가 수동으로 구축된 경우, 이벤트를 생성할 수 있습니다. 디바이스가 인라인에 위치한 경우, 악성 패

킷 또한 삭제할 수 있습니다. 시간 제한이 경과한 후 속도 상태가 중단될 경우, 이벤트 생성 및 패킷 삭제가 중지됩니다.

예를 들어 어느 한 IP 주소에서 최대 개수의 SYN 패킷을 허용하고, 해당 IP 주소에서 60초 동안 추가 연결을 차단하도록 설정을 구성할 수 있습니다.

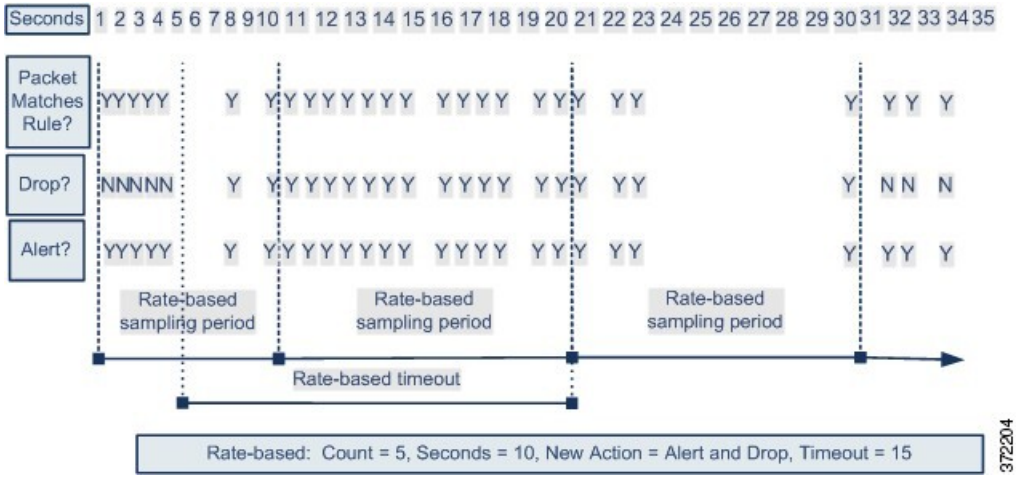
또한 네트워크에서 호스트를 오가는 TCP/IP 연결을 제한하여 서비스 거부 공격(DoS) 또는 사용자의 과도한 활동을 방지할 수 있습니다. 시스템이 특정 IP 주소 또는 주소 범위를 오가는 성공적인 연결의 구성된 수를 탐지하는 경우, 추가 연결에서 이벤트를 생성합니다. 속도 기반 이벤트 생성은 속도 조건의 발생 없이 시간 제한이 경과할 때까지 계속됩니다. 인라인 배포에서 속도 조건이 시간 초과될 때까지 패킷을 삭제하도록 선택할 수 있습니다.

예를 들어, 어느 것이든 하나의 IP 주소에서 최대 10개의 동시 연결이 성공할 수 있도록 설정을 구성할 수 있으며, 60초 동안 해당 IP 주소에서 추가 연결을 차단할 수 있습니다.

참고 내부 리소스에서의 디바이스 부하 균형 검사. 속도 기반 공격 방지를 설정할 때는 디바이스 단위가 아닌 리소스 단위로 트리거 속도를 설정해야 합니다. 속도 기반 공격 방지가 예상대로 작동하지 않는다면 트리거 속도를 줄여야 합니다. 사용자가 규정된 시간 간격 내에 너무 많은 연결 시도를 전송하면 알림이 트리거됩니다. 따라서 규칙의 속도를 제한하는 것이 좋습니다. 올바른 속도를 결정하는 데 어려움이 있다면 지원팀에 문의하십시오.

다음 다이어그램은 공격자가 호스트에 액세스하기 위해 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지가 구성된 규칙을 트리거합니다. 속도 기반 설정은 10초 범위 안에 규칙 일치가 다섯 번 발생하면 규칙 속성을 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 새로운 규칙 속성은 15초 후 시간 초과됩니다.

시간이 초과되더라도 패킷은 이어지는 속도 기반 샘플링 기간 내에 여전히 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 이벤트 생성으로 돌아갑니다.



관련 항목

동적 침입 규칙 상태

속도 기반 공격 방지 예시

`detection_filter` 키워드 및 임계값 설정 그리고 삭제 기능은 트래픽 자체 또는 시스템에서 생성된 이벤트를 필터링할 다른 방법을 제공합니다. 속도 기반 공격 차단을 단독으로 사용하거나 임계값 설정, 삭제, 또는 `detection_filter` 키워드를 조합하여 사용할 수 있습니다.

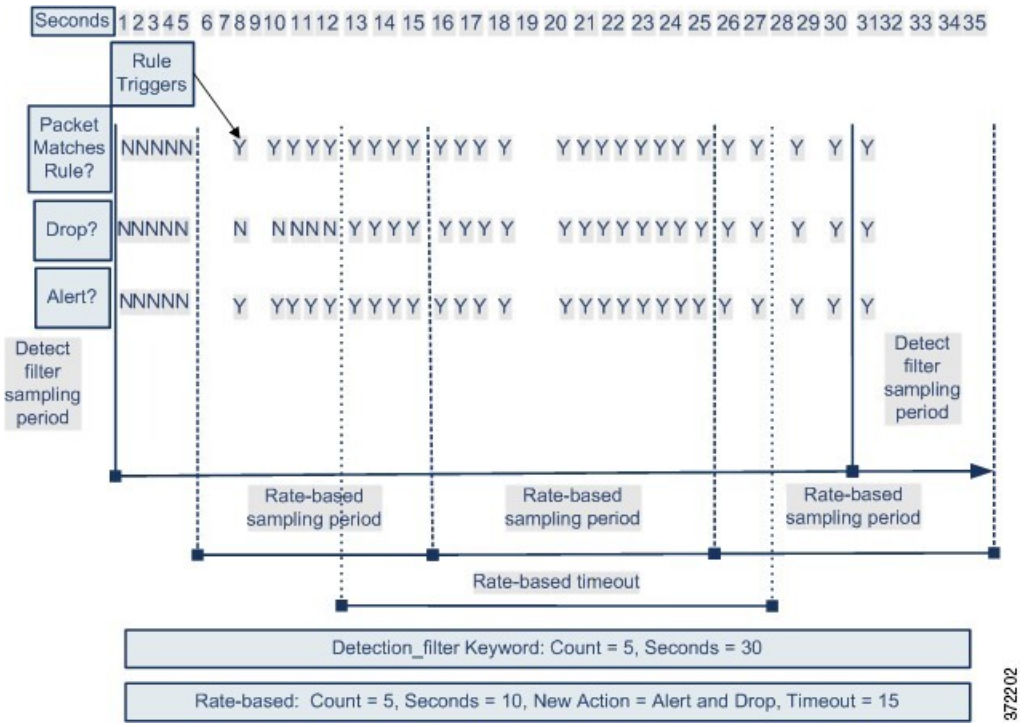
`detection_filter` 키워드, 임계값 설정 또는 억제, 속도 기반 기준 모두가 동일한 트래픽에 적용될 수도 있습니다. 규칙에 대한 삭제를 활성화하면, 속도 기반 변경이 발생한 경우에도 이벤트는 지정된 IP 주소에 대해 삭제됩니다.

detection_filter 키워드 예시

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 보여줍니다. 비밀번호를 찾는 반복된 시도는 또한 5로 설정된 계수와 함께 `detection_filter` 키워드를 포함하는 규칙을 트리거합니다. 이 규칙은 속도 기반 공격 방지가 설정되도록 합니다. 속도 기반 설정은 10초 범위 안에 규칙을 다섯 번 적중할 경우 규칙 속성을 20초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다.

다이어그램에 보여진 것과 같이, 속도가 `detection_filter` 키워드에 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 첫 5개의 패킷은 이벤트를 생성하지 않습니다. 규칙이 트리거되면 이벤트 알림이 시작되지만, 속도 기반 기준은 5개의 추가 패킷이 통과할 때까지 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하지 않습니다.

속도 기반 기준이 충족되면, 이벤트가 생성되고, 속도 기반 시간 제한이 만료되고 속도가 임계값 아래로 떨어질 때까지 패킷은 삭제됩니다. 20초가 지나면 속도 기반 작업이 시간 초과됩니다. 시간이 초과되더라도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 시간 제한이 발생할 때 샘플링된 속도는 이전 샘플링 기간의 임계값 속도보다 높으므로, 속도 기반 작업이 계속됩니다.



예제에는 이 내용이 없지만, Drop and Generate Events 규칙 상태를 `detection_filter` 키워드와 함께 사용하여 규칙에 대한 히트 수가 지정된 속도에 도달할 때 트래픽 삭제를 시작할 수 있습니다. 규칙에 대해 속도 기반 설정을 구성할 것인지 여부를 결정할 때는 규칙을 Drop and Generate Events(삭제 후 이벤트 생성)로 설정하고 `detection_filter` 키워드를 포함하는 경우 같은 결과가 생성되도록 할지, 아니면 침입 정책에서 속도 및 시간 초과 설정을 관리할지를 고려합니다.

관련 항목

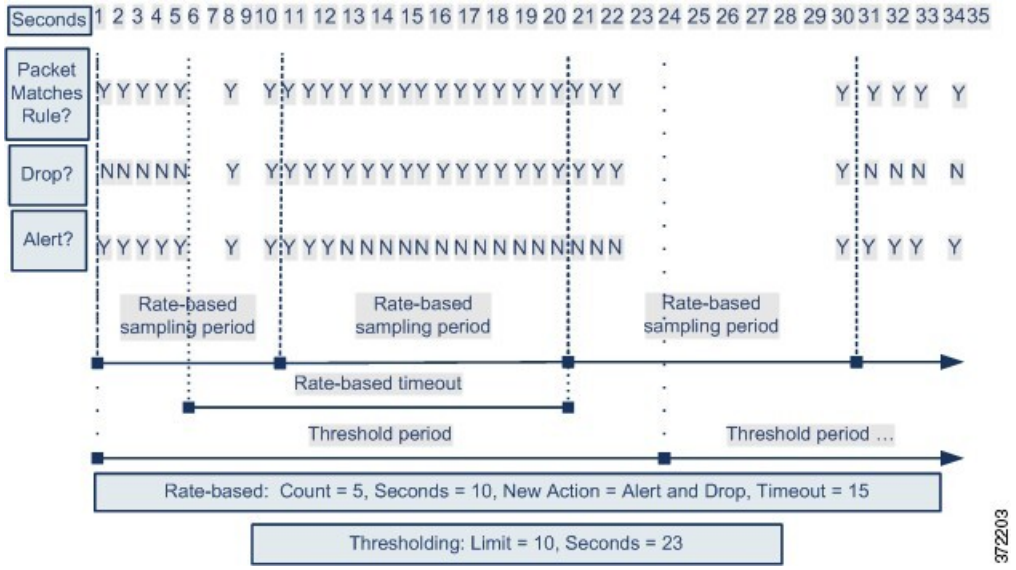
침입 규칙 상태

동적 규칙 상태 임계값 설정 및 삭제 예시

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지를 구성한 규칙을 트리거합니다. 속도 기반 설정은 10초 안에 규칙을 다섯 번 적중할 경우 규칙 속성을 15초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 또한, 제한 임계값은 규칙이 23초 안에 10개의 이벤트를 생성할 수 있도록 이벤트 수를 제한합니다.

다이어그램에 보여진 것과 같이, 규칙은 처음 5개의 일치 패킷의 이벤트를 생성합니다. 속도 기반 기준은 5개의 패킷 후 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하며, 다음 5개의 패킷 중에 규칙은 이벤트를 생성하고 시스템은 패킷을 삭제합니다. 10개의 패킷 후, 제한 임계값에 도달하므로, 나머지 패킷에 대해 시스템은 이벤트를 생성하지 않지만 패킷을 삭제합니다.

시간이 초과되더라도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 Generate Events(이벤트 생성)로 돌아갑니다.



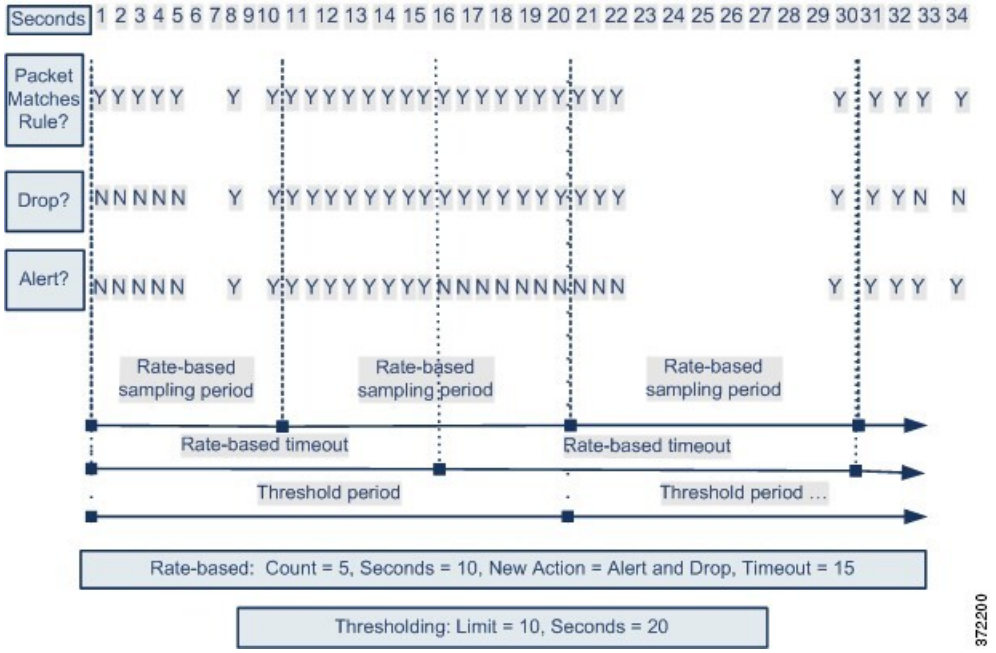
이 예에는 나와 있지 않지만, 임계값에 도달한 이후 속도 기반 기준 때문에 새 작업이 트리거되면 시스템은 작업 변화을 나타내는 단일 이벤트를 생성합니다. 따라서, 예를 들면, 제한 임계값인 10에 도달하고 시스템이 이벤트 생성을 중단하며 작업이 14번째 패킷에서 Drop and Generate Events(이벤트 삭제 및 생성)에서 Generate Events(이벤트 생성)로 변경되었을 때, 시스템은 작업 변화를 나타내는 11번째 이벤트를 생성합니다.

전정책적 속도 기반 탐지 및 임계값 설정 또는 삭제 예시

다음의 예시는 네트워크에서 호스트에 서비스 거부 공격(DoS) 공격을 시도한 공격자를 보여줍니다. 동일한 소스에서 호스트에 동시에 다수가 연결하면 정책 전반의 Control Simultaneous Connections(동시 연결 제어) 설정이 트리거됩니다. 설정은 10초 안에 한 개의 소스로부터 5개의 연결이 있을 때 이벤트를 생성하고 악성 트래픽을 삭제합니다. 또한, 전역 제한 임계값은 모든 규칙 또는 설정이 20초 안에 10개의 이벤트를 생성할 수 있도록 이벤트 수를 제한합니다.

다이어그램에 나와 있듯이, 정책 전반의 설정은 처음 10개의 일치 패킷에 대해 이벤트를 생성하고 트래픽을 삭제합니다. 10개의 패킷 후, 제한 임계값에 도달되므로, 나머지 패킷에 대한 어떤 이벤트도 생성되지 않지만 패킷이 삭제됩니다.

시간이 초과되더라도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 이벤트를 생성하고 트래픽을 삭제하는 속도 기반 작업은 계속됩니다. 속도 기반 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 중지됩니다.



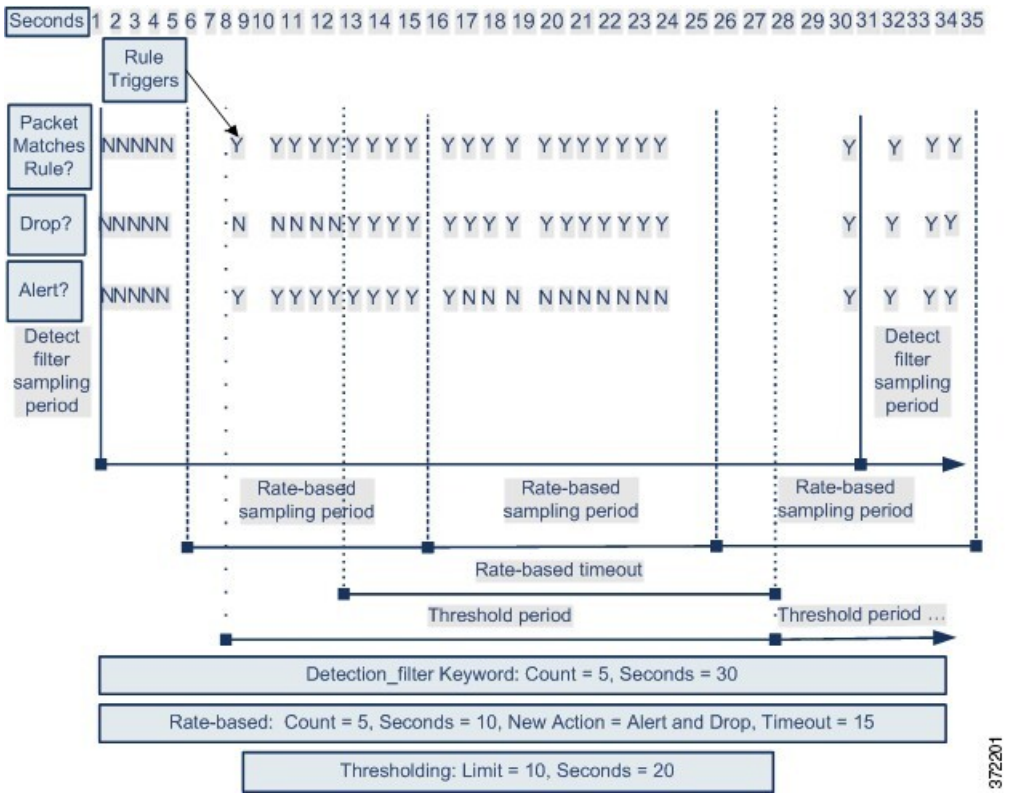
이 예에는 나와 있지 않지만, 임계값에 도달한 이후 속도 기반 기준 때문에 새 작업이 트리거되면 시스템은 작업 변화을 나타내는 단일 이벤트를 생성합니다. 따라서, 예를 들면, 제한 임계값인 10에 도달하고 시스템이 이벤트 생성을 중단하며 작업이 14번째 패킷에서 Drop and Generate Events(이벤트 삭제 및 생성)로 변경되었을 때, 시스템은 작업 변화를 나타내는 11번째 이벤트를 생성합니다.

여러 필터링 방법으로 속도 기반 탐지 예시

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 표시하고, `detection_filter` 키워드, 속도 기반 필터링, 임계값 설정이 상호 작용하는 경우에 대해 설명합니다. 비밀번호를 찾는 반복된 시도는 또한 5로 설정된 계수와 함께 `detection_filter` 키워드를 포함하는 규칙을 트리거합니다. 이 규칙에는 또한 15초 안에 다섯 번의 적중이 있을 경우 규칙 속성을 30초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경하는 속도 기반 공격 방지 설정이 있습니다. 또한, 제한 임계값은 규칙이 30초 안에 10개의 이벤트를 생성할 수 있도록 규칙을 제한합니다.

다이어그램에 표시된 대로 속도가 `detection_filter` 키워드에 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 첫 5개의 패킷은 이벤트 알림을 야기하지 않습니다. 규칙이 트리거되면 이벤트 알림이 시작되지만, 속도 기반 기준은 5개의 추가 패킷이 통과할 때까지 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하지 않습니다. 속도 기반 기준이 충족되면, 시스템은 패킷 11-15를 위한 이벤트를 생성하고 패킷을 삭제합니다. 15개의 패킷 후 제한 임계값에 도달하므로, 나머지 패킷에 대해 시스템은 이벤트를 생성하지 않지만 패킷을 중단합니다.

속도 기반 시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 이전 샘플링 기간의 임계값 속도보다 높으므로 새로운 작업이 계속됩니다.



속도 기반 공격 방지 옵션 및 구성

속도 기반 공격 방지는 잘못된 트래픽 패턴을 식별하고 정당한 요청에 대한 해당 트래픽의 영향을 최소화하려고 합니다. 속도 기반 공격은 일반적으로 다음 중 하나의 특성을 갖습니다.

- 네트워크의 호스트로 향하는 불완전한 연결을 포함하는, SYN 플러드 공격을 나타내는 모든 트래픽
- 네트워크의 호스트로 향하는 과도하고 완전한 연결을 포함하는, TCP/IP 연결 플러드 공격을 나타내는 모든 트래픽
- 특정 목적지 IP 주소 또는 주소로 이동하거나 특정 소스 IP 주소 또는 주소에서 오는 트래픽에서의 과도한 규칙 일치
- 모든 트래픽을 가로지르는 특정 규칙에 대한 과도한 일치 항목

네트워크 분석 정책에서 전체 정책에 대한 SYN flood 또는 TCP/IP 연결 flood 탐지를 구성할 수 있습니다. 침입 정책에서 개별적인 침입 또는 전처리기 규칙을 위한 속도 기반 필터를 설정할 수 있습니다. 수동으로 속도 기반 필터를 GID 135 규칙에 추가하거나 규칙 상태를 수정할 수는 없습니다. GID 135가 포함된 규칙은 해당 클라이언트를 소스 값으로 사용하고 해당 서버를 대상 값으로 사용합니다.

SYN Attack Prevention(SYN 공격 방지**)**이 활성화된 경우, 정의된 속도 조건이 초과되면 규칙 135:1이 트리거됩니다.

Control Simultaneous Connections(동시 연결 제어**)**가 활성화된 경우, 정의된 속도 조건이 초과되면 규칙 135:2가 트리거되고, 세션이 닫히거나 시간 초과되면 규칙 135:3이 트리거됩니다.

참고 내부 리소스에서의 디바이스 부하 균형 검사. 속도 기반 공격 방지를 설정할 때는 디바이스 단위가 아닌 리소스 단위로 트리거 속도를 설정해야 합니다. 속도 기반 공격 방지가 예상대로 작동하지 않는다면 트리거 속도를 줄여야 합니다. 사용자가 규정된 시간 간격 내에 너무 많은 연결 시도를 전송하면 알림이 트리거됩니다. 따라서 규칙의 속도를 제한하는 것이 좋습니다. 올바른 속도를 결정하는 데 어려움이 있다면 지원팀에 문의하십시오.

각 속도 기반 필터에는 여러 구성 요소가 포함되어 있습니다.

- 정책 전반 또는 규칙 기반 소스나 대상 설정을 위한 네트워크 주소 지정
- 특정 시간(초) 이내 규칙 일치의 계수로 구성한 규칙 일치 비율
- 속도가 초과될 때 수행할 새 작업

  전체 정책에 대한 속도 기반 설정을 설정한 경우, 시스템이 속도 기반 공격을 탐지하면 이벤트를 생성하고, 인라인 배포에서 트래픽을 삭제할 수 있습니다. 개별 규칙에 대한 속도 기반 작업을 설정할 때 Generate Events(이벤트 생성), Drop and Generate Events(이벤트 삭제 및 생성), Disable(비활성화)라는 세 가지 작업을 사용할 수 있습니다.

- 시간 제한 값으로 설정한 작업 기간

시작한 경우, 속도가 해당 기간 동안 구성된 속도까지 떨어지더라도 시간 제한에 도달할 때까지 새로운 작업이 발생한다는 점에 유의하십시오. 시간 제한이 만료되면, 속도가 임계값 아래로 떨어진 경우, 규칙 작업은 규칙에 처음 설정된 작업으로 돌아갑니다. 정책 전반 설정의 경우, 작업은 트래픽과 일치하는 각 규칙의 작업으로 돌아갑니다. 일치하는 규칙이 없는 경우 작업이 중지됩니다.

인라인 배포에서 속도 기반 공격 차단을 구성하여 일시적으로 또는 영구적으로 공격을 차단할 수 있습니다. 속도 기반 구성없이, Generate Events(이벤트 생성)로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙에 대한 패킷을 삭제하지 않습니다. 하지만 속도 기반 기준이 구성되어 있는 규칙이 공격 트래픽과 일치하는 경우, 해당 규칙이 처음에는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있지 않더라도 속도 작업은 속도 작업이 활성화된 기간 동안 패킷이 삭제되도록 할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나 비활성화된 규칙에 일치하는 트래픽을 삭제할 수 없습니다. 하지만 정책 수준에서 속도 기반 필터를 설정하는 경우, 지정된 기간 이내에 SYN 패킷 또는 SYN/ACK 상호작용의 과도한 수를 포함하는 트래픽에 이벤트를 생성하거나 트래픽에 이벤트를 생성하고 삭제할 수 있습니다.

동일한 규칙에서 다중 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 나열된 첫 번째 필터의 우선 순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌할 때 시스템은 첫 번째 속도 기반 필터의 작업을 시행합니다. 마찬가지로, 필터가 충돌하는 경우 정책 전반의 속도 기반 필터는 개별 규칙에 설정된 속도 기반 필터를 재정의합니다.

관련 항목

규칙 페이지에서 동적 규칙 상태 설정

속도 기반 공격 방지, 탐지 필터링 및 임계값 설정 또는 삭제

`detection_filter` 키워드는 지정된 시간 내에 규칙 일치의 임계값 수가 나올 때까지 규칙이 트리거되지 않게 합니다. 규칙이 `detection_filter` 키워드를 포함할 경우, 시스템은 시간 제한별 규칙에서 패턴 일치한 수신 패킷 수를 추적할 수 있습니다. 시스템은 특정 소스 또는 대상 IP 주소에서 해당 규칙 적중 횟수를 카운트할 수 있습니다. 속도가 규칙의 속도를 초과한 후, 해당 규칙에 대한 이벤트 알림이 시작됩니다.

임계값 설정 및 삭제를 사용하여 소스 또는 대상에 대한 이벤트 알림 수를 제한함으로써 또는 해당 규칙에 대한 알림을 모두 삭제함으로써 과도한 이벤트를 줄일 수 있습니다. 또한 특정 임계값을 재정의하지 않는 각 규칙에 적용되는 전역 규칙 임계값을 설정할 수도 있습니다.

규칙에 억제를 적용할 경우, 정책 전반 또는 규칙 단위의 속도 기반 설정 때문에 속도 기반 작업 변화가 발생하더라도 시스템은 모든 사용 가능한 IP 주소에 대해 해당 규칙의 이벤트 알림을 억제합니다.

관련 항목

침입 이벤트 임계값
침입 정책 삭제 구성
전역 규칙 임계값 기본 사항

속도 기반 공격 방지 구성

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

정책 수준에서 속도 기반 공격 차단을 구성하여 SYN 플러드 공격을 차단할 수 있습니다. 또한 특정 소스로부터 또는 특정 대상을 향한 과도한 연결을 중지할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 **3** 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 설정을 클릭합니다.

단계 **5** **Specific Threat Detection(**특정 위협 탐지**)**의 **Rate-Based Attack Prevention(**속도 기반 공격 방지**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **Rate-Based Attack Prevention(**속도 기반 공격 방지**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트를 초과하도록 고안된 불완전 연결을 차단하려면 **SYN Attack Prevention(SYN** 공격 방지**)** 아래의 **Add(**추가**)**를 클릭합니다.
- 과도한 수의 연결을 방지하려면 **Control Simultaneous Connections** 아래에서 **Add**를 클릭합니다.

단계 **8** 트래픽을 추적할 방법을 지정합니다.

- 특정 소스 또는 소스 범위에서 출발하는 모든 트래픽을 추적하려면 **Track By(**추적 기준**)** 드롭다운 목록에서 **Source(**소스**)**를 선택하고 **Network(**네트워크**)** 필드에 단일 IP 주소 또는 주소 블록을 입력합니다.
- 특정 대상 또는 대상 범위로 향하는 모든 트래픽을 추적하려면 **Track By(**추적 기준**)** 드롭다운 목록에서 **Destination(**대상**)**을 선택하고 **Network(**네트워크**)** 필드에 IP 주소 또는 주소 블록을 입력합니다.

참고

- 모든 서브넷 또는 IP를 모니터링하기 위해 Network(네트워크) 필드에 IP 주소 0.0.0.0/0을 입력하지 마십시오. 시스템은 속도 기반 공격 방지를 위해 이 IP 주소(일반적으로 모든 서브넷 또는 IP를 식별하는 데 사용됨)를 지원하지 않습니다.
- 시스템은 **Network(**네트워크**)** 필드에 포함된 각 IP 주소에 대한 개별 트래픽을 추적합니다. 구성한 속도 결과를 초과하는 단일 IP 주소로부터의 트래픽은 해당 IP 주소만을 위해 생성된 이벤트로 귀결됩니다. 한 예를 들어, 네트워크 구성에 `10.1.0.0/16`의 소스 CIDR 차단을 설정하고 10개의 동시 연결이 개방되어 있을 때 이벤트를 생성하도록 시스템을 구성할 수 있습니다. 10.1.4.21에서 8개의 연결이 열리고 10.1.5.10에서 6개의 연결이 열리는 경우, 어느 소스도 트리거하는 수의 연결을 갖고 있지 않으므로 시스템이 이벤트를 생성하지 않습니다. 그러나, 10.1.4.21에서 11개의 동시 연결이 열리는 경우, 시스템은 10.1.4.21로부터의 연결에 해당하는 이벤트만 생성합니다.

  시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **9** 속도 추적 설정의 시작 속도를 지정합니다.

- SYN 공격 설정의 경우에는 **Rate(**속도**)** 필드에 초당 SYN 패킷 수를 지정합니다.
- 동시 연결 설정의 경우에는 **Count(**계수**)** 필드에 연결 수를 입력합니다.

내부 리소스에서의 디바이스 부하 균형 검사. 속도 기반 공격 방지를 설정할 때는 디바이스 단위가 아닌 리소스 단위로 트리거 속도를 설정해야 합니다. 속도 기반 공격 방지가 예상대로 작동하지 않는다면 트리거 속도를 줄여야 합니다. 사용자가 규정된 시간 간격 내에 너무 많은 연결 시도를 전송하

면 알림이 트리거됩니다. 따라서 규칙의 속도를 제한하는 것이 좋습니다. 올바른 속도를 결정하는 데 어려움이 있다면 지원팀에 문의하십시오.

단계 **10** 속도 기반 공격 방지 설정에 일치하는 패킷을 삭제하려면 **Drop(**삭제**)** 확인란을 선택합니다.

단계 **11** **Timeout(**시간 초과**)** 필드에 SYN 일치 패턴이 있거나 동시 연결이 존재하는 트래픽에 대한 이벤트 생성(적용 가능한 경우에는 이벤트 삭제)까지 대기하는 시간을 입력합니다.

주의 높은 시간 제한 값을 설정하면 인라인 배포에서 호스트로 향하는 연결을 완전히 차단할 수 있습니다.

단계 **12** **OK(**확인**)**를 클릭합니다.

단계 **13** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축), Firepower Management Center 관리 가이드 참조.