전송 및 네트워크 레이어 전처리기

다음 주제에서는 전송 및 네트워크 계층 전처리기와 이를 구성하는 방법을 설명합니다.

전송 및 네트워크 계층 전처리기 소개

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

전송 및 네트워크 레이어 전처리기는 IP 조각을 이용한 공격을 탐지하고 체크섬 유효성 검증을 수행하며, TCP와 UDP 세션 전처리를 수행합니다. 패킷이 전처리기로 전달되기 전에, 패킷 디코더는 전처리기 및 침입 규칙 엔진에서 쉽게 사용할 수 있는 형식으로 패킷 헤더와 페이로드를 변환하고 패킷 헤더에서 다양한 이상 작업을 탐지합니다. 패킷을 디코딩한 후 다른 전처리기에 전송하기 전에 인라인 표준화 전처리기는 인라인 배포를 위해 트래픽을 표준화합니다.

침입 규칙 또는 규칙 인수에 비활성화된 전처리기가 필요한 경우, 네트워크 분석 정책의 웹 인터페이스에서 전처리기가 비활성화 상태로 남아 있더라도 시스템은 자동으로 전처리기를 현재 구성으로 사용합니다.

전송 및 네트워크 레이어 전처리기에 대한 라이선스 요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

전송 및 네트워크 계층 전처리기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

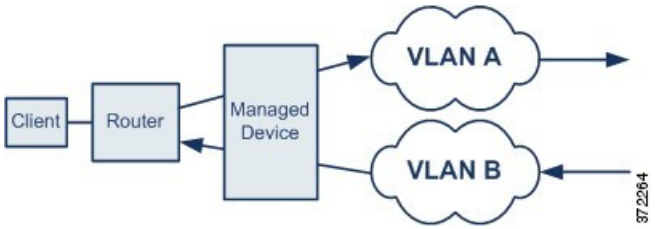
고급 전송/네트워크 전처리기 설정

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

고급 전송 및 네트워크 전처리 설정은 액세스 제어 정책을 배포하는 모든 네트워크, 영역 및 VLAN에 글로벌로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다.

무시된 VLAN 헤더

동일한 연결에 대해 다른 방향으로 이동하는 트래픽의 서로 다른 VLAN 태그는 트래픽 리어셈블리 및 규칙 처리에 영향을 줄 수 있습니다. 예를 들어 다음 그림에서는 동일한 연결에 대한 트래픽을 VLAN A를 통해 전송하고 VLAN B를 통해 수신할 수 있습니다.



패킷이 구축에 맞게 올바르게 처리될 수 있도록 시스템이 VLAN 헤더를 무시하게 설정할 수 있습니다.

침입 삭제 규칙에서의 활성 응답

드롭 규칙은 규칙 상태가 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 침입 또는 전처리기 규칙입니다. 인라인 배포에서 시스템은 트리거 패킷을 삭제하고 패킷이 시작된 세션을 차단하여 TCP 또는 UDP 드롭 규칙에 응답합니다.

팁 UDP 데이터 스트림은 일반적으로 세션의 측면에서 평가되지 않으므로 스트림 전처리기는 캡슐화 IP 데이터그램 헤더의 소스 및 대상 IP 주소 필드와 UDP 헤더의 포트 필드를 사용하여 흐름 방향을 결정하고 UDP 세션을 식별합니다.

하나 이상의 *active responses(*활성 응답*)*를 시작하도록 시스템을 구성하면 위반 패킷이 TCP 또는 UDP 삭제 규칙을 트리거할 때 더욱 정확하고 구체적츠로 TCP 연결 또는 UDP 세션을 닫을 수 있습니다. 활성 응답은 라우티드 및 투명 구축을 포함한 인라인 구축에서 사용할 수 있습니다. 활성 응답은 패시브 구축에는 적합하지 않으며 지원되지 않습니다.

활성 응답을 구성하려면 다음을 수행합니다.

- TCP 또는 UDP(**resp** 키워드만 해당) 침입 규칙을 생성하거나 수정합니다. 침입 규칙 헤더 프로토콜의 내용을 참조하십시오.
- **react** 또는 **resp** 키워드를 침입 규칙에 추가합니다. x활성 응답 키워드를 참조하십시오.
- TCP 연결의 경우 원한다면 전송할 추가 활성 응답의 최대 수와, 활성 응답 간 대기 시간(초)을 지정할 수 있습니다. 자세한 내용은 고급 전송/네트워크 전처리기 옵션, 4 페이지의 **Maximum Active Responses(**최대 활성 응답**)** 및 **Minimum Response Seconds(**최소 응답 시간 **(**초**))**를 참조하십시오.

활성 응답은 다음과 같은 일치하는 트래픽이 삭제 규칙을 트리거하면 세션을 닫습니다.

- **TCP** - 트리거 패킷을 삭제하고 클라이언트와 서버 트래픽 모두에 TCP Reset(RST) 패킷을 삽입합니다.

- **UDP** - ICMP 도달 불가 패킷을 세션의 각 끝 부분에 전송합니다.

고급 전송/네트워크 전처리기 옵션

연결을 추적할 때는 **VLAN** 헤더를 무시하십시오.

다음에서처럼 트래픽을 식별할 때 VLAN 헤더를 무시할지 포함할지를 지정합니다.

- 이 옵션을 선택하면 시스템은 VLAN 헤더를 무시합니다. 서로 다른 방향으로 이동하는 트래픽 내의 같은 연결에 대한 다른 VLAN 태그를 탐지하는, 구축된 디바이스에 이 설정을 사용하십시오.
- 이 옵션을 비활성화하면 시스템은 VLAN 헤더를 포함합니다. 서로 다른 방향으로 이동하는 트래픽 내의 같은 연결에 대한 다른 VLAN 태그를 탐지하지 않는, 구축된 디바이스에 이 설정을 사용하십시오.

최대 활성 응답

TCP 연결당 최대 활성 응답 수를 지정합니다. 추가 트래픽은 활성 응답이 시작된 연결에서 발생하고, 이전 활성 응답 이후 **Minimum Response Seconds(**최소 응답 시간**(**단위**:** 초**))**보다 트래픽이 더 많이 발생한 경우, 지정된 최대값에 도달하지 않는 한 시스템은 다른 활성 응답을 보냅니다. 0으로 설정하면 **resp** 또는 **react** 규칙이 트리거하는 추가 활성 응답이 비활성화됩니다. 침입 삭제 규칙에서의 활성 응답, 3 페이지 및 활성 응답 키워드를 참조하십시오.

트리거된 **resp** 또는 **react** 규칙은 이 옵션의 구성과 상관없이 활성 응답을 시작합니다.

최소 응답 시간**(**단위**:** 초**)**

Maximum Active Responses(최대 활성 응답**)**에 도달할 때까지, 시스템이 능동 응답을 시작한 연결에 대한 추가 트래픽이 후속 능동 응답으로 이어지기 전의 대기 시간(단위: 초)을 지정합니다.

문제 해결 옵션**:** 세션 종료 로깅 임계값

주의 지원팀의 지시가 있을 때만 세션 종료 로깅 임계값을 수정하십시오.

Support(지원팀)는 문제 해결 통화 중에 시스템을 구성하여 개별 연결이 지정된 임계값을 초과하면 메시지를 로깅하도록 요청할 수 있습니다. 이 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

이 옵션은 세션이 종료되고 지정된 수가 초과된 경우 로깅된 메시지의 바이트 수를 지정합니다.

참고 1GB의 상한 값은 또한 스트림 처리에 할당된 관리되는 디바이스의 메모리 양에 의해 제한됩니다.

관련 항목

활성 응답 키워드

고급 전송/네트워크 전처리기 설정

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

이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자여야 합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 수정할 정책에 대해 **Edit(**수정**)** ( )을 클릭합니다.

단계 **2** **More(**자세히**)** > **Advanced Settings(**고급 설정**)**를 클릭한 다음 **Transport/Network Preprocessor Settings(**전송/네트워크 전처리기 설정**)** 섹션 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** 문제 해결 옵션 **Session Termination Logging Threshold(**세션 종료 로깅 임계값**)**를 제외하고, 고급 전송/네트워크 전처리기 옵션, 4 페이지에서 설명하는 옵션을 수정합니다.

주의 지원팀의 지시가 있을 때만 **Session Termination Logging Threshold(**세션 종료 로깅 임계값**)**를 수정하십시오.

단계 **4** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 선택 사항으로, 액세스 제어 정책 수정에 설명된 대로 정책을 구성합니다.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

체크섬 확인

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

시스템은 프로토콜 수준 체크섬을 모두 검증하여 전체 IP, TCP, UDP 및 ICMP 전송이 수신되고 기본 수준에서 패킷이 전송 중에 함부로 조작되거나 실수로 변경되지 않았는지 확인할 수 있습니다. 체크섬은 알고리즘을 사용하여 패킷 내 프로토콜의 무결성을 확인합니다. 종단 호스트가 패킷 내에 작성한 것과 동일한 값을 시스템이 산출할 경우 패킷은 변경되지 않은 것으로 간주됩니다.

체크섬 확인을 비활성화한 경우 네트워크는 삽입 공격의 영향을 받기 쉽습니다. 시스템은 체크섬 확인 이벤트를 생성하지 않는다는 점에 유의하십시오. 인라인 배포에서 시스템을 구성하여 유효하지 않은 체크섬을 가진 패킷을 삭제할 수 있습니다.

체크섬 확인 옵션

수동 또는 인라인 배포에서 다음 옵션을 **Enabled(**활성화**)** 또는 **Disabled(**비활성화**)**로, 또는 인라인 배포에서 **Drop(**삭제**)**으로 설정할 수 있습니다.

- **ICMP** 체크섬
- **IP** 체크섬
- **TCP** 체크섬
- **UDP** 체크섬

옵션을 **Drop(**삭제**)**으로 설정하고 위반 패킷을 삭제하려면 관련 네트워크 분석 정책에서 **Inline Mode(**인라인 모드**)**를 활성화하고 장치가 인라인으로 구축되었는지 확인해야 합니다.

또한 이러한 옵션을 수동 배포에서 **Drop(**삭제**)**으로 설정하는 것은, 또는 탭 모드의 인라인 배포에서 그렇게 설정하는 것은 이들을 **Enabled(**활성화**)**로 설정하는 것과 동일합니다.

주의 **TCP** 체크섬에서 **Ignore(**무시**)** 옵션(기본값)은 구성된 모든 Snort 규칙을 우회하거나 무시합니다.

모든 체크섬 확인 옵션의 기본값은 **Enabled**입니다. 하지만 threat defense 라우팅 및 투명 인터페이스는 언제나 IP 체크섬 확인에 실패하는 패킷을 삭제합니다. threat defense 라우팅 및 투명 인터페이스는 배드 체크섬이 있는 UDP 패킷을 수정한 후 패킷을 Snort 프로세스로 전달합니다.

관련 항목

인라인 구축의 전처리기 트래픽 수정

체크섬 확인

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** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **Checksum Verification(**체크섬 확인**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **Checksum Verification(**체크섬 확인**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** 체크섬 확인, 5 페이지에 설명된 대로 옵션을 수정합니다.

참고 **TCP** 체크섬에서 **Ignore(**무시**)** 옵션(기본값)은 구성된 모든 Snort 규칙을 우회하거나 무시합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

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

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

인라인 정상화 전처리기

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

인라인 정상화 전처리기는 인라인 배포에서 공격자가 탐지를 우회하는 가능성을 최소화하기 위해 트래픽을 정상화합니다.

참고 시스템이 트래픽에 영향을 미치려면 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 관련 구성을 매니지드 디바이스에 구축해야 합니다.

IPv4, IPv6, ICMPv4, ICMPv6 및 TCP 트래픽의 모든 조합에 대해 표준화를 지정할 수 있습니다. 대부분의 표준화는 패킷 기준이며 인라인 표준화 전처리기에 의해 수행됩니다. 그러나 TCP 페이로드 표준화를 포함하여 대부분의 상태 관련 패킷 및 스트림 표준화는 TCP 스트림 전처리기가 처리합니다.

인라인 표준화는 패킷 디코더의 디코딩 직후 및 다른 전처리기의 처리 직전에 발생합니다. 표준화는 패킷 레이어의 내부에서 외부로 진행됩니다.

인라인 표준화 전처리기는 이벤트를 생성하지 않고 인라인 배포에서 다른 전처리기 및 규칙 엔진에 의한 사용을 위해 패킷을 준비합니다. 또한 전처리기를 통해 시스템이 처리하는 패킷이 네트워크 호스트에서 수신된 패킷과 동일한지 확인할 수 있습니다.

참고 인라인 배포에서는 인라인 모드를 활성화하고 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화된 인라인 표준화 전처리기를 구성할 것을 권장합니다. 수동 배포에서는 적응형 프로파일 업데이트을 사용하는 것이 좋습니다.

관련 항목

인라인 구축의 전처리기 트래픽 수정
적응형 프로파일 정보

인라인 표준화 옵션

최소 **TTL**

Reset TTL(TTL 재설정**)**이 이 옵션에 설정된 값보다 크거나 같을 때 다음을 지정합니다.

- **Normalize IPv4**가 활성화되었을 때 시스템이 IPv4 Time to Live (TTL) 필드에서 허용할 최소값. 값이 더 낮으면 TTL에 대한 패킷 값이 **Reset TTL**에 대해 설정된 값으로 표준화됩니다.
- **Normalize IPv6**이 활성화되었을 때 시스템이 IPv6 Hop Limit 필드에서 허용할 최소값. 값이 더 낮으면 Hop Limit에 대한 패킷 값이 **Reset TTL**에 대해 설정된 값으로 표준화됩니다.

필드가 비어 있는 경우 시스템은 값을 1로 가정합니다.

참고 threat defense 라우팅 및 투명 인터페이스의 경우 **Minimum TTL(**최소 **TTL)** 및 **Reset TTL(TTL** 재설정**)** 옵션은 무시됩니다. 연결에 대한 최대 TTL은 초기 패킷의 TTL이 결정합니다. 후속 패킷에 대한 TTL은 줄일 수는 있지만 늘릴 수는 없습니다. 시스템은 TTL을 해당 연결에 대해 목격된 최저 TTL로 재설정합니다. 이렇게 하면 TTL 회피 공격을 방지할 수 있습니다.

패킷 디코딩 **Detect Protocol Header Anomalies(**포로토콜 헤더 이상 탐지**)** 옵션이 활성화되면, 이 옵션을 위해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.에 대한 디코더 규칙 카테고리의 다음 규칙을 활성화할 수 있습니다.

- 규칙 116:428을 활성화하여 시스템이 지정된 최소 값보다 작은 TTL 값이 포함된 IPv4 패킷을 탐지하는 경우 트리거할 수 있습니다.
- 규칙 116:270을 활성화하여 시스템이 지정된 최소 값보다 작은 홉 제한 값이 포함된 IPv6 패킷을 탐지하는 경우 트리거할 수 있습니다.

TTL 재설정

Minimum TTL(최소 **TTL)**보다 크거나 같은 값을 설정할 때, 다음을 표준화합니다.

- **Normalize IPv4**가 활성화된 경우 IPv4 TTL 필드
- **Normalize IPv6**이 활성화된 경우 IPv6 Hop Limit 필드

패킷 값이 **Minimum TTL**보다 작은 경우 시스템은 TTL 또는 Hop Limit 값을 이 옵션에 대해 설정된 값으로 변경하여 패킷을 표준화합니다. 이 필드에 아무 값도 입력하지 않거나 0 또는 **Minimum TTL(**최소 **TTL)**보다 작은 값으로 설정하면 이 옵션이 비활성화됩니다.

IPv4 표준화

IPv4 트래픽의 표준화를 활성화합니다. 시스템은 다음 조건 시 필요하다면 TTL 필드도 표준화합니다.

- 이 옵션을 활성화하고,
- **Reset TTL(TTL** 재설정**)**에 설정된 값이 TTL 표준화를 활성화합니다.

이 옵션을 활성화하면 추가 IPv4 옵션도 활성화할 수 있습니다.

이 옵션을 활성화하면, 시스템은 다음 기본 IPv4 표준화를 수행합니다.

- 과도한 페이로드를 가진 패킷을 IP 헤더에 지정된 데이터그램 길이로 줄입니다.
- 예전에는 Type of Service(서비스 유형, ToS)로 알려졌던 Differentiated Services(차별화된 서비스, DS) 필드의 내용을 지웁니다.
- 모든 옵션 옥텟을 1(무연산)로 설정합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. Threat Defense 디바이스는 라우터 알림, 옵션 목록의 끝(EOOL), 특정 라우팅 또는 투명 인터페이스의 작업 없음(NOP)을 제외한 다른 IP 옵션을 포함하는 RSVP 패킷은 모두 삭제합니다.

조각화 금지 비트 표준화

IPv4 Flags(플래그) 헤더 필드의 단일 비트 Don't Fragment(조각화 금지) 하위 필드의 내용을 지웁니다. 이 옵션을 활성화하면 필요한 경우 다운스트림 라우터가 패킷을 삭제하는 대신 조각화할 수 있습니

다. 또한 삭제할 조작된 패킷에 기반하여 회피를 방지할 수 있습니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

예약 비트 표준화

IPv4 Flags(플래그) 헤더 필드의 단일 비트 Reserved(예약) 하위 필드의 내용을 지웁니다. 일반적으로 이 옵션을 활성화합니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

TOS 비트 표준화

예전에는 Type of Service(서비스 유형, ToS)로 알려졌던 1바이트 Differentiated Services(차별화된 서비스, DS) 필드의 내용을 지웁니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

초과 페이로드 표준화

페이로드가 과도한 패킷을 IP 헤더 및 Layer(레이어) 2(예를 들어, Ethernet(이더넷)) 헤더에 지정된 데이터그램 길이로 줄이지만 최소 프레임 길이 이하로 줄이지는 않습니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. 초과 페이로드가 있는 패킷은 이러한 인터페이스에서는 항상 삭제됩니다.

IPv6 표준화

Hop-by-Hop Options(홉 바이 홉 옵션) 및 Destination Options(대상 옵션) 확장 헤더의 모든 Option Type(옵션 유형) 필드를 00(건너뛰기 및 처리 계속)으로 설정합니다. 이 옵션이 활성화되고 **Reset TTL(TTL** 재설정**)**에 설정된 값이 홉 제한 표준화를 활성화하는 경우 시스템에서도 필요에 따라 Hop Limit(홉 제한) 필드를 표준화합니다.

ICMPv4 표준화

ICMPv4 트래픽 내 Echo(Request)(에코(요청)) 및 Echo Reply(에코 응답) 메시지에서 8비트 Code(코드) 필드의 내용을 지웁니다.

ICMPv6 표준화

ICMPv6 트래픽 내 Echo(Request)(에코(요청)) 및 Echo Reply(에코 응답) 메시지에서 8비트 Code(코드) 필드의 내용을 지웁니다.

예약 비트 표준화**/**지우기

TCP 헤더에 있는 Reserved(예약) 비트를 지웁니다.

옵션 패딩 바이트 표준화**/**지우기

모든 TCP 옵션 패딩 바이트를 지웁니다.

URG=0인 경우 긴급 포인터 지우기

긴급(URG) 제어 비트가 설정되지 않은 경우 16비트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드의 내용을 지웁니다.

빈 페이로드의 긴급 포인터**/URG** 지우기

페이로드가 없는 경우 TCP 헤더 Urgent Pointer(긴급 포인터) 필드의 내용 및 URG 제어 비트를 비웁니다.

긴급 포인터가 설정되지 않은 경우 **URG** 지우기

긴급 포인터가 설정되지 않은 경우 TCP 헤더 URG 제어 비트를 지웁니다.

긴급 포인터 표준화

포인터가 페이로드 길이보다 긴 경우 2바이트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드를 페이로드 길이로 설정합니다.

TCP 페이로드 표준화

TCP Data(데이터) 필드의 표준화를 활성화하여 재전송된 데이터의 일관성을 유지합니다. 제대로 리어셈블될 수 없는 모든 세그먼트는 삭제됩니다.

SYN 데이터 제거

TCP 운영 체제 정책이 Mac OS가 아닌 경우 동기화(SYN) 패킷의 데이터를 제거합니다.

또한 이 옵션은 TCP 스트림 전처리기 **Policy(**정책**)** 옵션이 **Mac OS**로 설정돼 있지 않을 때 트리거할 수 있는 규칙 129:2를 비활성화합니다.

RST 데이터 제거

TCP 재설정(RST) 패킷에서 모든 데이터를 제거합니다.

Window로 데이터 절감

TCP Data(데이터) 필드를 Window 필드에 지정된 크기로 줄입니다.

MSS로 데이터 절감

페이로드가 Maximum Segment Size(최대 세그먼트 크기, MSS)보다 긴 경우 TCP Data(데이터) 필드를 MSS로 줄입니다.

해결할 수 없는 **TCP** 헤더 이상 징후 차단

이 옵션을 활성화하면 표준화된 경우 시스템은 유효하지 않고 수신 호스트가 차단할 가능성이 높은 변칙적 TCP 패킷을 차단합니다. 예를 들어, 시스템은 설정된 세션에 차후에 전송된 모든 SYN 패킷을 차단합니다.

시스템은 또한 규칙이 활성화되어 있는지 여부에 관계없이 다음 TCP 스트림 전처리기 규칙에 하나라도 일치하는 모든 패킷을 삭제합니다.

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14~129:19

Total Blocked Packets(전체 차단된 패킷) 성능 표는 인라인 배포와 수동 배포 및 탭 모드의 인라인 배포에서 차단된 패킷 수 및 인라인 배포에서 차단되었을 수도 있는 수를 추적합니다.

명시적 정체 알림

Explicit Congestion Notification(명시적 정체 알림, ECN) 플래그의 패킷별 또는 스트림별 표준화를 다음과 같이 활성화합니다.

- 협상에 관계없이 패킷별로 ECN 플래그를 지우려면 **Packet(**패킷**)**을 선택합니다
- ECN 사용이 협상되지 않은 경우 스트림별로 ECN 플래그를 지우려면 **Stream(**스트림**)**을 선택합니다

Stream(스트림**)**을 선택한 경우, 이 표준화를 실행하려면 TCP 스트림 전처리기 **Require TCP 3-Way Handshake(TCP 3**방향 핸드셰이크 요청**)** 옵션을 활성화해야 합니다.

기존 **TCP** 옵션 지우기

Allow These TCP Options(이러한 **TCP** 옵션 허용**)**을 활성화합니다.

이러한 **TCP** 옵션 허용

사용자가 트래픽에서 허용하는 특정 TCP 옵션의 표준화를 비활성화합니다.

시스템은 사용자가 명시적으로 허용하는 옵션을 표준화하지 않습니다. 이는 옵션을 No Operation(무연산, TCP 옵션 1)으로 설정함으로써 사용자가 명시적으로 허용하지 않는 옵션을 표준화합니다.

시스템은 **Allow These TCP Options(**이러한 **TCP** 옵션 허용**)** 설정 여부에 상관없이 다음 옵션을 항상 허용해야 합니다. 최상의 TCP 성능을 위해 자주 사용하는 옵션이기 때문입니다.

- 최대 세그먼트 크기(MSS)
- 창 크기 조정
- 타임 스탬프 TCP

시스템은 드물게 사용되는 다른 옵션은 자동으로 허용하지 않습니다.

다음의 예시에서처럼 옵션 키워드, 옵션 번호, 또는 둘 다로 이루어진 쉼표로 구분된 목록을 작성하여 특정 옵션을 허용할 수 있습니다.

```
sack, echo, 19
```

옵션 키워드를 지정하는 것은 키워드와 관련된 하나 이상의 TCP 옵션을 지정하는 것과 같습니다. 예를 들어, `sack`을 지정하는 것은 TCP 옵션 4(Selective Acknowledgment Permitted(허용된 선택적 수신 확인)) 및 5(Selective Acknowledgment(선택적 수신 확인))를 지정하는 것과 같습니다. 옵션 키워드는 대소문자를 구분하지 않습니다.

또한 모든 TCP 옵션을 허용하고 모든 TCP 옵션의 표준화를 효과적으로 비활성화하는 `any`를 지정할 수 있습니다.

다음 표는 허용할 TCP 옵션을 지정하는 방법에 대해 요약합니다. 필드를 비워 둘 경우, 시스템은 MSS, Window Scale(Window 크기), Time Stamp(타임 스탬프) 옵션만 허용합니다.

지정 대상	허용 대상
sack	TCP 옵션 4(Selective Acknowledgment Permitted(허용된 선택적 수신 확인)) 및 5(Selective Acknowledgment(선택적 수신 확인))
echo	TCP 옵션 6(Echo Request(에코 요청)) 및 7(Echo Reply(에코 응답))
partial_order	TCP 옵션 9(Partial Order Connection Permitted(허용된 부분 순서 연결)) 및 10(Partial Order Service Profile(부분 순서 서비스 프로파일))
conn_count	TCP Connection Count(연결 집계) 옵션 11(CC), 12(CC.New(새로운)), 그리고 13(CC.Echo(에코))
alt_checksum	TCP 옵션 14(Alternate Checksum Request(대체 체크섬 요청)) 및 15(Alternate Checksum(대체 체크섬))
md5	TCP 옵션 19(MD5 서명)
옵션 번호. 2~255.	키워드가 없는 옵션을 비롯한 특정 옵션
any	모든 TCP 옵션. 이 설정은 TCP 옵션 표준화를 효과적으로 비활성화합니다

이 옵션에 `any`를 지정하지 않은 경우, 표준화에는 다음이 포함됩니다.

- MSS, Window Scale(Window 크기), Time Stamp(타임 스탬프) 및 모든 명시적으로 허용된 옵션을 제외하고, 모든 옵션 바이트를 No Operation(무연산, TCP 옵션 1)으로 설정합니다.
- Time Stamp(타임 스탬프)가 존재하지만 유효하지 않은 경우, 또는 유효하지만 협상되지 않은 경우, Time Stamp(타임 스탬프) 옥텟을 No Operation(무연산)으로 설정합니다.
- Time Stamp(타임 스탬프)가 협상되었지만 존재하지 않는 경우 패킷을 차단합니다.

- Acknowledgment(수신 확인, ACK) 제어 비트가 설정되지 않은 경우 Time Stamp Echo Reply(타임스탬프 에코 응답, TSecr) 옵션 필드를 비웁니다.
- SYN 제어 비트가 설정되지 않은 경우 MSS 및 Window Scale(Window 크기) 옵션을 No Operation(무연산, TCP 옵션 1)으로 설정합니다

인라인 표준화 설정

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

시작하기 전에

- 위반 패킷을 표준화 또는 삭제하려면 인라인 구축의 전처리기 트래픽 수정에 설명된 대로 **Inline Mode(**인라인 모드**)**를 활성화합니다. 또한 매니지드 디바이스는 인라인으로 구축해야 합니다.

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(캐럿이 아니라 단어를 클릭).

단계 **5** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **Inline Normalization(**인라인 표준화**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **Inline Normalization(**인라인 표준화**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** 인라인 정상화 전처리기, 7 페이지에 설명된 대로 옵션을 설정합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- 인라인 표준화 Minimum TTL(최소 TTL) 옵션이 침입 이벤트를 생성하게 하려면, 패킷 디코더 규칙 116:429(IPv4)와 116:270 (IPv6) 중 하나 또는 둘 다를 활성화합니다. 자세한 내용은 침입 규칙 상태 설정 및 인라인 표준화 옵션, 8 페이지를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

IP 조각 모음 전처리기

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

IP 데이터그램이 최대 전송 단위(MTU)보다 커서 2개 이상의 소규모 IP 데이터그램으로 쪼개진 경우 조각화됩니다. 단일 IP 데이터그램 조각에는 숨겨진 공격을 식별하기에 충분한 정보가 포함되어 있지 않을 수 있습니다. 공격자는 조각화된 패킷 내에 공격 데이터를 전송하여 탐지 우회를 시도할 수 있습니다. IP 조각 모음 전처리기는 규칙 엔진이 조각화된 IP 데이터그램에 대해 규칙을 실행하기 전에 이를 리어셈블하므로 규칙이 해당 패킷에서 공격을 더욱 적절히 식별할 수 있습니다. 조각화된 데이터그램이 리어셈블되지 않는 경우 데이터그램에 대해 규칙이 실행되지 않습니다.

IP 단편화 익스플로잇

IP 조각 모음을 활성화하면 티어드롭 공격과 같은 네트워크 호스트에 대한 공격 및 Jolt2 공격과 같은 시스템 자체에 대한 리소스 소모 공격을 탐지할 수 있습니다.

티어드롭 공격은 특정 운영 체제에서 버그를 공격하는데, 중첩되는 IP 조각을 리어셈블하려고 시도할 때 충돌을 야기합니다. IP 조각 모음 전처리기가 중첩되는 조각을 식별하도록 활성화 및 구성된 경우 이를 수행합니다. IP 조각 모음 전처리기는 티어드롭과 같은 중첩되는 조각화 공격의 첫 번째 패킷을 탐지하지만 동일한 공격의 후속 패킷은 탐지하지 않습니다.

Jolt2 공격은 IP 조각 모음기를 혹사시키기 위한 시도로 동일한 조각화된 IP 패킷을 엄청난 수로 복제하여 전송해서 DoS(Denial-of-Service) 공격을 야기합니다. 메모리 사용량 한도는 IP 조각 모음 전처리기에서 이것 및 이와 유사한 공격을 차단하고, 철저한 검사를 기반으로 시스템 자체 보호를 유지합니다. 시스템은 공격에 의해 마비되지 않고 운영 상태를 유지하며 계속해서 네트워크 트래픽을 검사합니다.

다양한 운영 체제는 조각화된 패킷을 다양한 방법으로 리어셈블합니다. 호스트가 실행 중인 운영 체제를 결정할 수 있는 공격자는 또한 악성 패킷을 조각화하여 대상 호스트가 특정 방식으로 이를 리어셈블하도록 할 수 있습니다. 모니터링한 네트워크 상의 호스트가 어떤 운영 체제를 실행 중인지 시스템에서 알 수 없기 때문에 전처리기가 패킷을 부정확하게 검사하고 리어셈블할 수 있으므로 익스플로잇이 탐지되지 않고 통과될 수 있습니다. 이러한 유형의 공격을 줄이기 위해 조각 모음 전처리기를 네트워크의 각 호스트에 대한 패킷을 조각 모음하는 적절한 방법을 사용하도록 구성할 수 있습니다.

또한 수동 구축에서 적응형 프로파일 업데이트을(를) 사용하여 패킷의 대상 호스트에 대한 호스트 운영체제 정보를 통해 IP 조각 모음 전처리기의 대상 기반 정책을 동적으로 선택할 수도 있습니다.

대상 기반 조각 모음 정책

호스트의 운영체제는 다음과 같은 3가지 기준을 바탕으로, 패킷을 리어셈블리할 때 우선해야 할 패킷 프래그먼트를 결정합니다.

- 운영체제가 프래그먼트를 수신한 순서
- 패킷의 오프셋(패킷 시작 부분에서 프래그먼트까지의 거리(단위: 바이트))
- 중첩 프래그먼트 대비 패키의 시작 위치와 마지막 위치

모든 운영 체제가 이러한 기준을 사용하지만, 조각화된 패킷을 리어셈블할 때 서로 다른 운영 체제는 서로 다른 조각을 지원합니다. 따라서, 네트워크에서 서로 다른 운영 체제를 사용 중인 두 호스트는 중첩되는 동일한 조각을 완전히 다른 방법으로 리어셈블할 수 있습니다.

사용 중인 호스트 중 하나의 운영 체제를 알고 있는 공격자는 중첩되는 패킷 조각에 숨겨진 악성 콘텐츠를 전송하여 탐지 우회를 시도하고 해당 호스트를 공격할 수 있습니다. 이 패킷은 리어셈블되고 검사될 때는 무해하게 보일 수 있지만 대상 호스트에 의해 리어셈블될 경우에는 악성 익스플로잇이 포함됩니다. 그러나, 모니터링된 네트워크 세그먼트에서 실행되는 운영 체제를 식별하기 위해 IP 조각 모음 전처리기를 구성한 경우, 이는 대상 호스트가 하는 것과 동일한 방법으로 조각을 리어셈블하여 공격을 식별할 수 있습니다.

IP 조각 모음 옵션

단순히 IP 조각 모음을 활성화하거나 비활성화하도록 선택할 수도 있습니다. 그러나 Cisco는 IP 조각 모음 전처리기의 활성화된 작업을 더욱 세밀한 수준으로 지정할 것을 권장합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

다음 전역 옵션을 설정할 수 있습니다.

Preallocated Fragments(미리 할당된 조각**)**

전처리기가 한 번에 처리할 수 있는 개별 조각의 최대 수입니다. 미리 할당할 조각 노드의 수를 지정하면 정적 메모리 할당이 활성화됩니다.

주의 개별 조각을 처리하면 메모리 중 약 1550바이트가 사용됩니다. 전처리기가 개별 조각을 처리하는 데 관리되는 디바이스에 미리 정해진 허용 가능한 메모리 제한보다 더 많은 메모리가 필요한 경우 해당 디바이스의 메모리 제한이 우선합니다.

각 IP 조각 모음 정책에 다음 옵션을 구성할 수 있습니다,

네트워크

조각 모음 정책을 적용할 호스트의 IP 주소입니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255개의 프로파일을 지정할 수 있습니다.

참고 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.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

정책

모니터링된 네트워크 세그먼트의 호스트 집합에 사용할 조각 모음 정책입니다.

대상 호스트의 운영체제에 따라 7가지 조각 모음 정책 중 하나를 선택하면 됩니다. 다음 표는 7개의 정책 및 각각을 사용하는 운영 체제를 나열합니다. First 및 Last 정책 이름은 해당 정책이 원래의 중첩 패킷을 지원하는지, 아니면 후속 중첩 패킷을 지원하는지 여부를 반영합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

표 *1:* 대상 기반 조각 모음 정책

정책	운영 체제
BSD	AIX FreeBSD IRIX VAX/VMS
BSD-right	HP JetDirect

정책	운영 체제
First	Mac OS HP-UX
Linux	Linux OpenBSD
Last	Cisco IOS
Solaris	SunOS
(Windows용)	(Windows용)

시간 초과

조각화된 패킷을 리어셈블할 때 전처리기 엔진이 사용할 수 있는 최대 시간(단위: 초)을 지정합니다. 패킷이 지정된 기간 내에 리어셈블될 수 없는 경우, 전처리기 엔진은 패킷 리어셈블 시도를 중지하고 수신한 조각을 삭제합니다.

최소 **TTL**

패킷이 가질 수 있는 허용 가능한 최소 TTL 값을 지정합니다. 이 옵션은 TTL 기반 삽입 공격을 탐지합니다.

규칙 123:11을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

이상 징후 탐지

중첩되는 조각과 같은 조각화 문제를 식별합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

다음 규칙을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

- 123:1~123:4
- 123:5(BSD 정책)
- 123:6~123:8

중첩 제한

한 세션에서 중첩되는 세그먼트에 대해 구성된 수가 탐지된 경우 해당 세션에 대한 조각 모음이 중단됨을 명시합니다.

이 옵션을 구성하려면 **Detect Anomalies(**이상 징후 탐지**)**를 활성화해야 합니다. 빈 필드 값이 이 옵션을 비활성화합니다. 0 값은 무제한 중첩 세그먼트 수를 지정합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. 중첩되는 프래그먼트는 이러한 인터페이스에서는 항상 삭제됩니다.

규칙 123:12를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

최소 조각 크기

구성된 바이트 수보다 작은, 마지막이 아닌 조각이 탐지된 경우 패킷이 악성으로 간주됨을 명시합니다.

이 옵션을 구성하려면 **Detect Anomalies(**이상 징후 탐지**)**를 활성화해야 합니다. 빈 필드 값이 이 옵션을 비활성화합니다. 0 값은 무제한 바이트 수를 지정합니다.

규칙 123:13을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

IP 조각 모음 구성

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

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.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정를 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** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **IP Defragmentation(IP** 조각 모음**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **IP Defragmentation(IP** 조각 모음**)** 옆에 있는 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **7** 원한다면 **Preallocated Fragments(**미리 할당된 프래그먼트**)** 필드에 값을 입력합니다.

단계 **8** 다음 옵션을 이용할 수 있습니다.

- 서버 프로파일 추가 - 패널 왼쪽의 **Servers(**서버**)** 옆에 있는 **Add(**추가**)** (+)을 클릭하고, **Host Address(**호스트 주소**)** 필드에 값을 입력한 다음 **OK(**확인**)**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255가지 대상 기반 정책을 생성할 수 있습니다.
- 서버 프로파일 편집 - 패널 왼쪽의 **Servers(**서버**)**에서 설정한 주소를 클릭하거나 **default(**기본값**)**를 클릭합니다.
- 프로파일 삭제 - 정책 옆에 있는 **Delete(**삭제**)** (🗑)을 클릭합니다.

단계 **9** IP 조각 모음 옵션, 16 페이지에 설명된 대로 옵션을 수정합니다.

단계 **10** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 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.하려면 IP 조각 모음 규칙 (GID 123)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정 및 IP 조각 모음 옵션, 16 페이지의 내용을 참조하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 기본 사항
충돌 및 변경: 네트워크 분석 및 침입 정책

패킷 디코더

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

시스템은 전처리기에 캡처된 패킷을 보내기 전에 먼저 패킷 디코더에 패킷을 보냅니다. 패킷 디코더는 패킷 헤더와 페이로드를 전처리기 및 규칙 엔진이 쉽게 사용할 수 있는 형식으로 변환합니다. 각 스택 레이어는 데이터 링크 레이어에서 시작해서 네트워크 및 전송 레이어에 이르기까지 계속해서 차례로 디코딩됩니다.

패킷 디코더 옵션

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

GTP 데이터 채널 디코딩

캡슐화된 GTP(GPRS[General Packet Radio Service] 터널링 프로토콜) 데이터 채널을 디코딩합니다. 기본적으로, 디코더는 포트 3386의 버전 0 데이터 및 포트 2152의 버전 1 데이터를 디코딩합니다. `GTP_PORTS` 기본 변수를 사용하여 캡슐화된 GTP 트래픽을 식별하는 포트를 수정할 수 있습니다.

규칙 116:297 및 116:298을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

비표준 포트에서 **Teredo** 탐지

포트 3544 이외의 UDP 포트에서 확인된 IPv6 트래픽의 Teredo 터널링을 검사합니다.

IPv6 트래픽이 있으면 항상 시스템에서 검사합니다. 기본적으로, IPv6 검사에는 4in6, 6in4, 6to4 및 6in6 터널링 체계가 포함되며, UDP 헤더가 포트 3544를 지정하는 경우에는 Teredo 터널링도 포함됩니다.

IPv4 네트워크에서 IPv4 호스트는 Teredo 프로토콜을 사용하여 IPv4 NAT(Network Address Translation) 디바이스를 통해 IPv6 트래픽을 터널링할 수 있습니다. Teredo는 IPv4 NAT 디바이스의 배후에 있는 IPv6 연결을 허용하기 위해 IPv4 UDP 데이터그램 안에서 IPv6 패킷을 캡슐화합니다. 시스템은 일반적으로 UDP 포트 3544를 사용하여 Teredo 트래픽을 식별합니다. 그러나 공격자는 탐지를 피하기 위해 비표준 포트를 사용할 수 있습니다. **Detect Teredo on Non-Standard Ports(**비표준 포트에서 **Teredo** 탐지**)**를 활성화하여 시스템이 Teredo 터널링의 모든 UDP 페이로드를 검사하도록 할 수 있습니다.

Teredo 디코딩은 첫 번째 UDP 헤더에서만, 그리고 IPv4가 외부 네트워크 레이어에 사용될 때만 수행됩니다. IPv6 데이터에서 캡슐화된 UDP 데이터로 인해 Teredo IPv6 레이어 다음에 두 번째 UDP 레이어가 나타나는 경우 규칙 엔진은 UDP 침입 규칙을 사용하여 내부 및 외부 UDP 레이어를 분석합니다.

정책-기타 규칙 카테고리의 침입 규칙 12065, 12066, 12067 및 12068은 Teredo 트래픽을 탐지하지만 디코딩하지는 않는다는 점에 유의하십시오. 필요에 따라 이러한 규칙을 사용하여 인라인 구축에서 Teredo 트래픽을 삭제할 수 있습니다. 하지만 **Detect Teredo on Non-Standard Ports(**비표준 포트에서 **Teredo** 탐지**)**를 활성화할 때는 이러한 규칙이 비활성화되어 있거나 트래픽을 삭제하지 않고 이벤트를 생성하도록 설정되어 있는지 확인해야 합니다.

과도한 길이 값 탐지

패킷 헤더가 실제 패킷 길이보다 큰 패킷 길이를 지정할 때를 탐지합니다.

이 옵션은 threat defense 라우팅, 투명 및 인라인 인터페이스에 대해서는 무시됩니다. 헤더 길이가 너무 긴 패킷은 항상 삭제됩니다. 그러나 이 옵션은 threat defense 인라인 탭과 수동 인터페이스에는 적용되지 않습니다.

규칙 116:6, 116:47, 116:97 및 116:275를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

유효하지 않은 **IP** 옵션 탐지

유효하지 않은 IP 옵션을 사용하는 익스플로잇을 식별하기 위해 유효하지 않은 IP 헤더 옵션을 탐지합니다. 예를 들어, 시스템을 마비시키는 방화벽에 대한 DoS(Denial-of-Service) 공격이 존재합니다. 방화벽은 유효하지 않은 Timestamp(타임 스탬프) 및 Security IP(보안 IP) 옵션의 분석을 시도하고 제로 길이를 점검하는 데 실패하는데, 이는 복구할 수 없는 무한 루프를 야기합니다. 규칙 엔진은 제로 길이 옵션을 식별하고, 방화벽에서 공격을 완화하는 데 사용할 수 있는 정보를 제공합니다.

Threat Defense 디바이스는 라우터 알림, 옵션 목록의 끝(EOOL), 특정 라우팅 또는 투명 인터페이스의 작업 없음(NOP)을 제외한 다른 IP 옵션을 포함하는 RSVP 패킷은 모두 삭제합니다. 인라인, 인라인 탭 또는 수동 인터페이스의 경우 IP 옵션은 위에서 설명한 대로 처리됩니다.

규칙 116:4 및 116:5를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

실험적 **TCP** 옵션 탐지

실험적 TCP 옵션이 포함된 TCP 헤더를 탐지합니다. 다음 표는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
9	허용된 부분 순서 연결
10	부분 순서 서비스 프로파일
14	대체 체크섬 요청
15	대체 체크섬 데이터
18	트레일러 체크섬
20	우주 통신 프로토콜 표준(SCPS)
21	선택적 부정적 수신 확인(SCPS)
22	레코드 경계(SCPS)
23	손상(SPCS)
24	SNAP
26	TCP 압축 필터

이는 실험적 옵션이므로, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다.

참고 위 표에 나열된 실험적 옵션 외에도, 시스템은 26보다 큰 옵션 번호를 가진 모든 TCP 옵션을 실험적인 것으로 고려합니다.

규칙 116:58을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

사용하지 않는 **TCP** 옵션 탐지

사용하지 않는 TCP 옵션이 포함된 TCP 헤더를 탐지합니다. 이는 사용하지 않는 옵션이므로, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 다음 표는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
6	에코
7	에코 응답
16	Skeeter
17	Bubba
19	MD5 서명
25	지정되지 않음

규칙 116:57을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

T/TCP 탐지

CC.ECHO 옵션이 포함된 TCP 헤더를 탐지합니다. CC.ECHO 옵션은 TCP for Transactions(트랜잭션용 TCP, T/TCP)가 사용되고 있음을 확인합니다. T/TCP 헤더 옵션은 널리 사용되지 않기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다.

규칙 116:56을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

기타 **TCP** 옵션 탐지

다른 TCP 디코딩 이벤트 옵션으로 탐지되지 않는 유효하지 않은 TCP 옵션을 통해 TCP 헤더를 탐지합니다. 예를 들어, 이 옵션은 정확하지 않은 길이 또는 옵션 데이터를 TCP 헤더 외부에 배치하는 길이를 가진 TCP 옵션을 탐지합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다. 잘못된 TCP 옵션이 있는 패킷은 항상 삭제됩니다.

규칙 116:54, 116:55 및 116:59를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

프로토콜 헤더 이상 징후 탐지

더 많은 특정 IP 및 TCP 디코더 옵션으로 탐지되지 않는 다른 디코딩 오류를 탐지합니다. 예를 들어 디코더는 잘못된 형식의 데이터 연결 프로토콜 헤더를 탐지할 수 있습니다.

이 옵션은 threat defense 라우팅, 투명 및 인라인 인터페이스에 대해서는 무시됩니다. 헤더 이상 징후가 있는 패킷은 항상 삭제됩니다. 그러나 이 옵션은 Threat Defense(위협 방어) 인라인 탭과 수동 인터페이스에는 적용되지 않습니다.

이 옵션을 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 다음 규칙 중 하나를 활성화해야 합니다.

GID: SID	다음 경우에 이벤트를 생성합니다.
116:467	패킷이 Cisco FabricPath 헤더로 캡슐화한 패킷의 최소 크기보다 작습니다.
116:468	헤더의 CMD(Cisco Meta Data) 필드에 유효한 CMD 헤더의 최소 크기보다 작은 헤더 길이가 포함되어 있습니다. CMD 필드는 Cisco Trustsec 프로토콜과 연결됩니다.
116:469	헤더의 CMD 필드에 잘못된 필드 길이가 포함되어 있습니다.
116:470	헤더의 CMD 필드에 잘못된 SGT(Security Group Tag, 보안 그룹 태그) 옵션 유형이 있습니다.
116:471	헤더의 CMD 필드에 예약한 값이 있는 SGT가 포함되어 있습니다.

또한 다른 패킷 디코더 옵션과 연결되지 않은 패킷 디코더 규칙은 무엇이든 활성화할 수 있습니다.

관련 항목

사전 정의된 기본 변수

패킷 복호화 구성

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** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **Packet Decoding(**패킷 디코딩**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **Packet Decoding(**패킷 디코딩**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** 패킷 디코더 옵션, 21 페이지에 설명된 대로 옵션을 활성화 또는 비활성화합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 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.하려면 패킷 디코더 규칙 (GID 116)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정 및 패킷 디코더 옵션, 21 페이지의 내용을 참조하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 기본 사항
충돌 및 변경: 네트워크 분석 및 침입 정책

TCP 스트림 전처리

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

TCP 프로토콜은 연결이 존재할 수 있는 다양한 상태를 정의합니다. 각 TCP 연결은 소스 및 대상 IP 주소와 소스 및 대상 포트에 의해 식별됩니다. TCP는 동일한 연결 매개 변수 값을 가진 연결이 한 번에 하나만 존재하도록 허용합니다.

상태 관련 **TCP** 익스플로잇

침입 규칙에 `established` 인수로 `flow` 키워드를 추가한 경우, 침입 규칙 엔진은 상태 저장 모드에서 규칙 및 지시와 일치하는 패킷을 검사합니다. 상태 저장 모드는 클라이언트와 서버 사이의 적정 3방향 핸드셰이크로 설정된 TCP 세션의 일부인 트래픽만 평가합니다.

전처리기가 설정된 TCP 세션의 일부로 식별할 수 없는 모든 TCP 트래픽을 검색하도록 시스템을 구성할 수 있습니다. 그러나 이벤트가 시스템의 빠른 과부하를 야기하고 의미 있는 데이터를 제공하지 않으므로 일반적인 사용에는 권장되지 않습니다.

stick 및 snot과 같은 공격은 시스템의 광범위한 규칙 집합 및 자체 패킷 검사를 사용합니다. 이 도구는 Snort 기반 침입 규칙의 패턴에 따라 패킷을 생성하고, 네트워크를 통해 전송합니다. 사용자 규칙이 상태 저장 검사를 위한 규칙 구성을 위해 `flow` 또는 `flowbits` 키워드를 포함하지 않은 경우, 각 패킷은 규칙을 트리거하여 시스템을 마비시킵니다. 이러한 패킷은 설정된 TCP 세션의 일부가 아니며 의미 있는 정보를 제공하지 않으므로 상태 저장 검사를 통해 패킷을 무시할 수 있습니다. 상태 저장 검사를 수행하는 경우, 규칙 엔진은 설정된 TCP 세션의 일부인 해당 공격만 탐지하므로 분석가가 stick 또는 snot으로 인해 발생하는 이벤트 볼륨이 아닌 해당 공격에 집중할 수 있습니다.

대상 기반 **TCP** 정책

서로 다른 운영 체제는 TCP를 서로 다른 방식으로 구현합니다. 예를 들어, Windows 및 일부의 다른 운영 체제에서 세션을 재설정하려면 정확한 TCP 시퀀스 번호를 지닌 TCP 재설정 세그먼트가 필요한 반면, Linux 및 기타 운영 체제에서는 다양한 시퀀스 번호를 허용합니다. 이 예제에서, 스트림 전처리기는 대상 호스트가 시퀀스 번호에 근거한 재설정에 대응하는 방식을 정확하게 이해해야 합니다. 스트림 전처리기는 대상 호스트가 재설정을 유효한 것으로 간주하는 경우에 한해 세션 추적을 중지하므로, 전처리기가 스트림 검사를 중지한 후 공격이 패킷을 전송하여 탐지를 우회할 수 없습니다. TCP 구현의 다른 변경 사항에는 운영 체제가 TCP 타임 스탬프 옵션을 채택하는지 여부 등이 포함되 있으며, 이를 포함할 경우 타임 스탬프를 처리하는 방식 및 운영 체제가 SYN 패킷의 데이터를 수락하거나 무시하는지 여부를 포함합니다.

다양한 운영 체제는 또한 중첩되는 TCP 세그먼트를 다양한 방법으로 리어셈블합니다. 중첩되는 TCP 세그먼트는 접수되지 않은 일반 재전송을 반영할 수 있습니다. 세그먼트는 또한 호스트 중 하나의 운영 체제를 알고 있는 공격자가 중첩되는 세그먼트에 숨겨진 악성 콘텐츠를 전송하여 탐지를 우회하고 해당 호스트를 공격하는 시도를 나타낼 수 있습니다. 그러나, 스트림 전처리기를 구성하여 모니터링된 네트워크 세그먼트에서 실행되는 운영 체제를 인식할 수 있으며, 따라서 이는 대상 호스트가 하는 것과 동일한 방법으로 세그먼트를 리어셈블하여 공격을 식별하도록 허용합니다.

하나 이상의 TCP 정책을 만들어서 TCP 스트림 검사 및 리어셈블리를 모니터링된 네트워크 세그먼트에서 다른 운영 체제로 조정할 수 있습니다. 각 정책에 대해 13개 운영 체제 정책 중 하나를 확인합니다. 다른 운영 체제를 사용하는 호스트의 일부 또는 전체를 식별하기 위해 필요한 만큼 많은 TCP 정책을 사용하여 각 TCP 정책을 특정 IP 주소 또는 주소 블록에 바인딩합니다. 기본 TCP 정책은 다른 TCP 정책에서 식별하지 않는 모니터링된 네트워크의 모든 호스트에 적용되므로 기본 TCP 정책에 대한 IP 주소 또는 주소 블록을 지정할 필요가 없습니다.

또한 수동 구축에서 적응형 프로파일 업데이트을(를) 사용하여 패킷의 대상 호스트에 대한 호스트 운영체제 정보를 통해 TCP 스트림 전처리기의 대상 기반 정책을 동적으로 선택할 수도 있습니다.

TCP 스트림 리어셈블리

스트림 전처리기는 TCP 세션의 서버-클라이언트 통신 스트림, 클라이언트-서버 통신 스트림, 또는 둘 다에 속하는 모든 패킷을 수집하고 리어셈블합니다. 이를 통해 규칙 엔진은 주어진 스트림에 속하는 개별 패킷만 검사하는 것이 아니라 단일, 리어셈블된 엔터티로서의 스트림을 검사할 수 있습니다.

규칙 엔진은 스트림 리어셈블리를 통해 개별 패킷 검사에서는 탐지하지 못할 수 있는 스트림 기반 공격을 식별할 수 있습니다. 규칙 엔진이 네트워크의 필요에 따라 리어셈블할 통신 스트림을 지정할 수 있습니다. 예를 들어, 사용자 웹 서버에서 트래픽을 모니터링하는 경우에는 본인의 웹 서버로부터 악성 트래픽을 수신할 가능성이 거의 없으므로 클라이언트 트래픽만 검사하기를 원할 수 있습니다.

각 TCP 정책에서 스트림 전처리기가 리어셈블할 트래픽을 식별하는, 쉼표로 구분된 포트 목록을 지정할 수 있습니다. 적응형 프로파일 업데이트을(를) 활성화하는 경우, 포트에 대한 대안으로 또는 포트와 조합하여 리어셈블할 트래픽을 식별하는 서비스를 나열할 수 있습니다.

포트, 서비스, 또는 둘 다를 지정할 수 있습니다. 클라이언트 포트, 서버 포트 및 둘 다의 모든 조합에 대해 포트의 개별 목록을 지정할 수 있습니다. 또한 클라이언트 서비스, 서버 서비스 및 둘 다의 모든 조합에 대해 서비스의 개별 목록을 지정할 수 있습니다. 예를 들어 다음을 리어셈블하기를 원하는 것으로 가정합니다.

- 클라이언트로부터의 SMTP(포트 25) 트래픽
- FTP 서버 응답(포트 21)
- 두 방향 모두에서의 텔넷(포트 23) 트래픽

다음을 구성할 수 있습니다.

- 클라이언트 포트에 대해, `23, 25`를 지정합니다.
- 서버 포트에 대해, `21, 23`을 지정합니다.

또는, 그 대신, 다음을 설정할 수 있습니다.

- 클라이언트 포트에 대해, `25`를 지정합니다.
- 서버 포트에 대해, `21`을 지정합니다.
- 두 포트 모두에 대해, `23`을 지정합니다.

또한 포트 및 서비스를 결합하고 적응형 프로파일 업데이트을(를) 활성화하는 경우 유효하게 될 다음 예를 고려하십시오.

- 클라이언트 포트에 대해, `23`을 지정합니다.
- 클라이언트 서비스에 대해, `smtp`를 지정합니다.
- 서버 포트에 대해, `21`을 지정합니다.
- 서버 서비스에 대해, `telnet`을 지정합니다.

포트를 무효화(예: `!80`)하면 TCP 스트림 전처리기가 해당 포트에 대한 트래픽 처리를 차단하여 성능을 높일 수 있습니다.

모든 포트에 대해 리어셈블리를 제공하려면 `all`을 인수로 지정할 수도 있지만, 그렇게 하면 이 전처리기에서 검사하는 트래픽의 양이 증가하여 불필요하게 성능이 저하될 수 있으므로 Cisco는 포트를 `all`로 설정하는 것을 권장하지 않습니다.

TCP 리어셈블리는 다른 전처리기에 추가한 포트를 자동으로 포함합니다. 그러나, 다른 전처리기 구성에 추가한 TCP 리어셈블리 목록에 포트를 명확하게 추가한 경우, 이러한 추가 포트는 정상적으로 처리됩니다. 여기에는 다음 전처리기를 위한 포트 목록이 포함됩니다.

- FTP/Telnet(서버 수준 FTP)
- DCE/RPC
- HTTP 검사
- SMTP
- 세션 시작 프로토콜
- POP
- IMAP
- SSL

추가 트래픽 유형(클라이언트, 서버, 둘 다)을 리어셈블하면 리소스 요구가 증대된다는 점에 유의하십시오.

TCP 스트림 전처리 옵션

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

다음 전역 TCP 옵션을 구성할 수 있습니다.

패킷 유형 성능 증대

활성화된 침입 규칙에 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 TCP 트래픽 무시를 활성화합니다. 단, 소스 및 목적지 포트가 모두 `any`로 설정된 TCP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 예외입니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다.

각 TCP 정책에 대해 다음 옵션을 구성할 수 있습니다.

네트워크

사용자가 TCP 스트림 리어셈블리 정책을 적용할 호스트 IP 주소를 지정합니다.

단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 비롯한 255개의 총 프로파일을 지정할 수 있습니다.

참고 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.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

정책

대상 호스트의 TCP 정책 운영 체제를 식별합니다. **Mac OS** 이외의 정책을 선택하는 경우, 시스템은 동기화(SYN) 패킷에서 데이터를 제거하고 규칙 129:2의 이벤트 생성을 비활성화합니다. 인라인 표준화 전처리기 **Remove Data on SYN(SYN**에서 데이터 제거**)** 옵션을 활성화하면 규칙 129:2도 비활성화됩니다.

다음 표는 각각을 사용하는 호스트 운영 체제 및 운영 체제 정책을 식별합니다.

표 ***2: TCP*** 운영 체제 정책

정책	운영 체제
First	알 수 없는 OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 커널 Linux 2.6 커널
이전 Linux	Linux 2.2 및 이전 커널
(Windows용)	Windows 98 Windows NT Windows 2000 Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista

정책	운영 체제
Solaris	Solaris OS SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 이상
HPUX 10	HP-UX 10.2 이하
Mac OS	Mac OS 10(Mac OS X)

팁 First 운영 체제 정책에서는 호스트 운영 체제를 알 수 없는 경우 일부 보호를 제공할 수 있습니다. 하지만, 이로 인해 공격이 누락될 수 있습니다. 알고 있는 경우 정확한 운영 체제를 지정하는 정책을 수정해야 합니다.

시간 초과

1에서 86400 사이의 시간(단위: 초)으로, 침입 규칙 엔진이 이 시간 동안 상태 표에서 비활성 스트림을 유지합니다. 스트림이 지정된 시간에 리어셈블되지 않는 경우, 침입 규칙 엔진은 이를 상태 표에서 삭제합니다.

참고 관리되는 디바이스가 네트워크 트래픽이 디바이스의 대역폭 제한에 도달할 가능성이 높은 세그먼트에 구축된 경우, 처리 오버헤드의 양을 낮추기 위해 이 값을 더 높게(예: 600초) 설정할 것을 고려해야 합니다.

threat defense 디바이스는 이 옵션을 무시하며, 대신 고급 액세스 컨트롤 **Threat Defense Service Policy(**위협 방어 서비스 정책**)**의 설정을 사용합니다. 자세한 내용은 서비스 정책 규칙 구성를 참조하십시오.

최대 **TCP** 창

수신 호스트가 지정한 대로 허용된 1에서 1073725440바이트 사이의 최대 TCP 창 크기를 지정합니다. 값을 0으로 설정하면 TCP 창 크기 확인이 비활성화됩니다.

주의 상한은 RFC에서 허용하는 최대 창 크기이며 공격자의 탐지 회피를 방지하는 것이 목적이지만, 최대 창 크기를 너무 크게 설정하면 자체적으로 서비스 거부가 발생할 수 있습니다.

Stateful Inspection Anomalies(상태 저장 검사 이상 징후**)**가 활성화되면 이 옵션에 대해 규칙 129:6을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

중첩 제한

세션에서 중첩되는 세그먼트에 대해 0(무제한)과 255 사이의 구성된 번호가 탐지된 경우 해당 세션을 위한 세그먼트 리어셈블리가 중단되며, **Stateful Inspection Anomalies(**상태 저장 검사 이상 징후**)**가 활성화되고 동반되는 전처리기 규칙이 활성화된 경우 이벤트가 생성된다는 것을 지정합니다.

규칙 129:7을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

플러시 배율

인라인 구축에서, 비감소 크기의 세그먼트 1~2048 사이로 구성된 수에 이어 감소 크기의 세그먼트가 탐지된 경우 시스템은 탐지를 위해 누적된 세그먼트 데이터를 플러시합니다. 값을 0으로 설정하면 이러한 세그먼트 패턴의 탐지가 비활성화되며, 이는 요청 또는 응답의 종료를 나타낼 수 있습니다. 이 옵션을 적용하려면 Inline Normalization(인라인 표준화) **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화되어야 한다는 점에 유의하십시오.

상태 저장 검사 이상 징후

TCP 스택에서 비정상적 상태를 탐지합니다. TCP/IP 스택이 잘못 로깅된 경우 동반되는 전처리기 규칙이 활성화되면 이로 인해 많은 이벤트가 생성될 수 있습니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

다음 규칙을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

- 129:1~129:5
- 129:6(Mac OS만 해당)
- 129:8~129:11
- 129:13~129:19

다음에 유의하십시오.

- 규칙 129:6이 트리거되려면 **Maximum TCP Window(**최대 **TCP** 창**)**에 0보다 큰 값을 구성해야 합니다.
- 규칙 129:9 및 129:10이 트리거되려면 **TCP Session Hijacking(TCP** 세션 가로채기**)**도 활성화해야 합니다.

TCP 세션 가로채기

세션에서 수신된 후속 패킷에 대한 3방향 핸드셰이크 동안 TCP 연결의 양쪽에서 탐지된 하드웨어(MAC) 주소를 검증하여 TCP 세션 가로채기를 탐지합니다. 한쪽 또는 다른 쪽의 MAC 주소가 일치하지 않으면, **Stateful Inspection Anomalies**가 활성화되고 두 개의 해당 프리프로세서 규칙 중 하나가 활성화된 경우 시스템이 이벤트를 생성합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

규칙 129:9 및 129:10을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 이러한 규칙 중 하나가 이벤트를 생성하려면 **Stateful Inspaction Anomalies(**상태 저장 검사 이상 징후**)**도 활성화해야 합니다.

연속된 소규모 세그먼트

Stateful Inspection Anomalies가 활성화된 경우, 허용되는 연속 소형 TCP 세그먼트의 최대 수를 1~2048 범위로 지정합니다. 값을 0으로 설정하면 소규모 연속 세그먼트 확인이 비활성화됩니다.

이 옵션은 **Small Segment Size(**소규모 세그먼트 크기**)** 옵션과 함께 설정해야 합니다. 둘 다 비활성화하거나 둘 다 0이 아닌 값으로 설정합니다. 각 세그먼트의 길이가 1바이트라고 해도 개입 ACK 없이 최대 2000개의 연속 세그먼트를 수신하는 경우 일반적으로 예상하는 것보다 훨씬 많은 연속 세그먼트일 수 있음에 유의하십시오.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

규칙 129:12를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

소규모 세그먼트 크기

Stateful Inspection Anomalies가 활성화된 경우, 소형으로 간주되는 1~2048바이트의 TCP 세그먼트 크기를 지정합니다. 값을 0으로 설정하면 소규모 세그먼트의 크기가 비활성화됩니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

이 옵션은 **Consecutive Small Segment Size(**연속된 소규모 세그먼트 크기**)** 옵션과 함께 설정해야 합니다. 둘 다 비활성화하거나 둘 다 0이 아닌 값으로 설정합니다. 2048바이트 TCP 세그먼트는 일반적인 1500바이트 이더넷 프레임보다 크다는 점에 유의하십시오.

Ports Ignoring Small Segments(소규모 세그먼트를 무시하는 포트**)**

Stateful Inspection Anomalies(상태 저장 검사 이상 징후**)**, **Consecutive Small Segment Size(**연속된 소규모 세그먼트**)** 및 **Small Segment Size(**소규모 세그먼트 크기**)**가 활성화된 경우, 소규모 TCP 세그먼트 탐지를 무시하는 쉼표로 구분된 하나 이상의 포트 목록을 지정합니다. 이 옵션을 비워 두면 어떤 포트도 무시되지 않습니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

어느 포트든 목록에 추가할 수 있지만, 목록은 TCP 정책 내 **Perform Stream Reassembly on(**스트림 리어셈블리 수행**)** 포트 목록 중 하나에서 지정된 포트에만 영향을 미칩니다.

TCP 3방향 핸드셰이크 요청

TCP 3방향 핸드셰이크가 완료되는 경우에만 세션을 설정된 것으로 처리하도록 지정합니다. 성능을 향상시키고, SYN 플러드 공격으로부터 보호하며, 부분 비동기 환경에서 작업을 허용하려면 이 옵션을 비활성합니다. 설정된 TCP 세션의 일부가 아닌 정보를 전송하여 잘못된 긍정을 생성하려고 시도하는 공격을 차단하려면 이 옵션을 활성화합니다.

규칙 129:20을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

3방향 핸드셰이크 시간 제한

Require TCP 3-Way Handshake(TCP 3방향 핸드셰이크 요청**)**가 활성화된 경우 핸드셰이크 완료 기한이 되는 시간(단위: 초)을 0(무제한)에서 86400(24시간)까지의 범위에서 지정합니다. 이 옵션의 값을 수정하려면 **Require TCP 3-Way Handshake(TCP 3**방향 핸드셰이크 요청**)**를 활성화해야 합니다.

Firepower Software 디바이스 및 threat defense 인라인, 인라인, 패시브 인터페이스의 경우, 기본값은 0입니다. threat defense 라우팅 및 투명 인터페이스의 경우, 시간 초과는 항상 30 초이며, 여기서 구성된 값은 무시됩니다.

패킷 크기 성능 증대

전처리기가 리어셈블리 버퍼에서 대규모 패킷을 큐에 넣지 않도록 설정합니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다. 1~20바이트의 소규모 패킷을 사용하여 회피 시도를 차단하려면 이 옵션을 비활성화합니다. 모든 트래픽이 매우 큰 패킷으로 구성되어 있어서 그러한 공격이 없을 것임을 확신하는 경우 이 옵션을 활성화합니다.

레거시 리어셈블리

패킷을 리어셈블할 때 스트림 전처리기가 더 이상 사용되지 않는 Stream 4(스트림 4) 전처리기를 모방하도록 설정하여 스트림 전처리기가 리어셈블한 이벤트를 Stream 4(스트림 4) 전처리기가 리어셈블한 동일 데이터 스트림에 기반한 이벤트와 비교할 수 있습니다.

비동기 네트워크

모니터링된 네트워크가 비동기 네트워크, 즉, 시스템이 트래픽의 절반만 표시하는 네트워크인지 여부를 지정합니다. 이 옵션을 활성화할 경우, 시스템은 성능을 높이기 위해 TCP 스트림을 리어셈블하지 않습니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

클라이언트 포트에서 스트림 리어셈블리 수행

연결의 클라이언트 측 포트에 기반한 스트림 리어셈블리를 활성화합니다. 다시 말해, 일반적으로 $HOME_NET에 지정된 IP 주소에 의해 정의되는 웹 서버, 메일 서버, 또는 다른 IP 주소로 전송되는 스트림을 리어셈블합니다. 악성 트래픽이 클라이언트에서 시작될 것으로 예상되는 경우 이 옵션을 사용하십시오.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

클라이언트 서비스에서 스트림 리어셈블리 수행

연결의 클라이언트 측을 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 악성 트래픽이 클라이언트에서 시작될 것으로 예상되는 경우 이 옵션을 사용하십시오.

선택한 각 클라이언트 서비스에 대해 하나 이상의 클라이언트 탐지기가 활성화되어야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 연결된 클라이언트 애플리케이션에 활성화된 탐지기가 없는 경우, 시스템은 해당 애플리케이션의 모든 Cisco 제공 탐지기를 자동으로 활성화합니다. 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 해당 애플리케이션의 사용자 정의 탐지기를 활성화합니다.

이 기능을 사용하려면 보호 및 제어 라이선스가 필요합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

서버 포트에서 스트림 리어셈블리 수행

연결의 서버 측만을 위한 포트에 기반한 스트림 리어셈블리를 활성화합니다. 다시 말해, 일반적으로 $EXTERNAL_NET에 지정된 IP 주소에 의해 정의되는 웹 서버, 메일 서버, 또는 다른 IP 주소에서 시작되는 스트림을 리어셈블합니다. 서버 측 공격을 경계하고자 하는 경우 이 옵션을 사용합니다. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

참고 철저한 서비스 검사를 위해서는 Perform Stream Reassembly on Server Ports(서버 포트에서 스트림 리어셈블리 수행) 필드에 포트 번호를 추가하는 것 외에도 Perform Stream Reassembly on Server Services(서버 서비스에서 스트림 리어셈블리 수행) 필드에 서비스 이름을 추가합니다. 예를 들어 Perform Stream Reassembly on Server Ports(서버 포트에서 스트림 리어셈블리 수행) 필드에 포트 번호 80을 추가하는 것 외에도 Perform Stream Reassembly on Server Services(서버 서비스에서 스트림 리어셈블리 수행) 필드에 **'HTTP'** 서비스를 추가합니다.

서버 서비스에서 스트림 리어셈블리 수행

연결의 서버 측만을 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 서버 측 공격을 경계하고자 하는 경우 이 옵션을 사용합니다. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

하나 이상의 탐지기를 활성화해야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 서비스에 활성화된 탐지기가 없는 경우, 시스템은 연결된 애플리케이션 프로토콜의 모든 Cisco 제공 탐지기를 자동으로 활성화합니다. 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 애플리케이션 프로토콜의 사용자 정의 탐지기를 활성화합니다.

이 기능을 사용하려면 보호 및 제어 라이선스가 필요합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

두 포트 모두에서 스트림 리어셈블리 수행

연결의 클라이언트 및 서버 측 모두를 위한 포트에 기반한 스트림 리어셈블리를 활성화합니다. 동일한 포트의 악성 트래픽이 클라이언트와 서버 사이에서 어느 방향에서나 이동할 수 있을 것으로 예상되는 경우 이 옵션을 사용하십시오. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

두 서비스 모두에서 스트림 리어셈블리 수행

연결의 클라이언트 및 서버 측 모두를 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 동일한 서비스의 악성 트래픽이 클라이언트와 서버 사이에서 어느 방향에서나 이동할 수 있을 것으로

예상되는 경우 이 옵션을 사용하십시오. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

하나 이상의 탐지기를 활성화해야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 연결된 클라이언트 애플리케이션 또는 애플리케이션 프로토콜에 대해 활성화된 탐지기가 없을 경우 해당 애플리케이션 또는 애플리케이션 프로토콜에 대해 자동으로 모든 Cisco 제공 탐지기가 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션 또는 애플리케이션 프로토콜에 대해 활성화됩니다.

이 기능을 사용하려면 보호 및 제어 라이선스가 필요합니다.

이 옵션은 threat defense 라우팅 및 투명 인터페이스에 대해서는 무시됩니다.

문제 해결 옵션: 최대 대기 바이트

Support(지원팀)는 문제 해결 통화 중 사용자에게 TCP 연결의 한 쪽에 대기될 수 있는 데이터의 양을 지정하도록 요청할 수 있습니다. 0 값은 무제한 바이트 수를 지정합니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

문제 해결 옵션: 최대 대기 세그먼트

Support(지원팀)는 문제 해결 통화 중 사용자에게 TCP 연결의 한 쪽에 대기될 수 있는 세그먼트의 최대 바이트 수를 지정하도록 요청할 수 있습니다. 0 값은 무제한 데이터 세그먼트 바이트 수를 지정합니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

관련 항목

탐지기 활성화 및 비활성화
레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

TCP 스트림 전처리 구성

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

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.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정를 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 NAT 정책 옆의 **Edit(**수정**)** ( )을 클릭합니다.

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

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

단계 **5** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **TCP Stream Configuration(TCP** 스트림 설정**)** 설정이 비활성화되어 있다면 **Enabled(**활성화**)**를 클릭해 활성화합니다.

단계 **6** **TCP Stream Configuration(TCP** 스트림 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** **Global Settings(**전역 설정**)** 섹션의 **Packet Type Performance Boost(**패킷 유형 성능 증대**)** 확인란을 선택하거나 선택 취소합니다.

단계 **8** 다음 작업을 수행할 수 있습니다.

- 대상 기반 정책 추가 - Targets(대상) 섹션의 **Hosts(**호스트**)** 옆에 있는 **Add(**추가**)** ( )를 클릭합니다. **Host Address(**호스트 주소**)** 필드에 하나 이상의 IP 주소를 지정합니다. 단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255가지 대상 기반 정책을 생성할 수 있습니다. 완료되면 **OK(**확인**)**를 클릭합니다.
- 기존 대상 기반 정책 편집 - **Hosts(**호스트**)**에서 편집할 정책의 주소를 클릭하거나, default(기본값)를 클릭해 기본 설정값을 편집합니다.
- TCP Stream Preprocessing(TCP 스트림 전처리) 옵션을 수정합니다(TCP 스트림 전처리 옵션, 28 페이지 참조).

  주의 지원팀이 지시할 때만 **Maximum Queued Bytes(**최대 대기 바이트**)** 또는 **Maximum Queued Segments(**최대 대기 세그먼트**)**를 수정하십시오.

팁 클라이언트, 서버 또는 두 서비스를 기반으로 스트림 리어셈블리 설정을 수정하려면 수정할 필드 내부를 클릭하거나 필드 옆에 있는 **Edit(편집)**를 클릭합니다. 화살표를 이용하여 팝업 창의 **Available(사용 가능)** 및 **Enabled(활성화)** 목록에서 서비스를 이동한 다음 **OK(확인)**를 클릭합니다.

- 기존 대상 기반 정책 삭제 - 제거할 정책 옆에 있는 **Delete(삭제)** ( )를 클릭합니다.

단계 **9** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(정책 정보)**을 클릭한 다음 **Commit Changes(변경 사항 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 TCP Stream(TCP 스트림) 전처리기 규칙(GID 129)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정 및 TCP 스트림 전처리 옵션, 28 페이지의 내용을 참조하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

UDP 스트림 전처리

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

UDP 스트림 전처리는 규칙 엔진이 다음 인수 중 하나를 사용하여 `flow` 키워드를 포함하는 UDP 규칙에 대해 패킷을 처리할 때 발생합니다.

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP 데이터 스트림은 세션의 측면에서는 일반적으로 고려되지 않습니다. UDP는 커뮤니케이션 채널을 설정하고, 데이터를 교환하며, 채널을 종료하는 두 엔드포인트를 위한 수단을 제공하지 않는 비연결형 프로토콜입니다. 그러나, 스트림 전처리기는 흐름의 방향을 결정하고 세션을 확인하기 위해 캡슐화하는 IP 데이터그램 헤더의 소스 및 대상 IP 주소 필드, 그리고 UDP 헤더의 포트 필드를 사용합니다. 구성 가능한 타이머가 초과되는 경우, 또는 둘 중 한 쪽의 엔드포인트가 다른 엔드포인트에 도달할 수 없거나 요청된 서비스가 사용할 수 없다는 ICMP 메시지를 수신한 경우 세션이 종료됩니다.

시스템이 UDP 스트림 전처리와 관련된 이벤트를 생성하지 않는다는 점에 유의하십시오. 하지만, 관련된 패킷 디코더 규칙을 활성화하여 UDP 프로토콜 헤더 이상 징후를 탐지할 수 있습니다.

관련 항목

TCP 헤더 값 및 스트림 크기

UDP 스트림 전처리 옵션

시간 초과

전처리기가 상태 표에서 비활성 스트림을 유지하는 시간(단위: 초)을 지정합니다. 추가 데이터그램이 지정된 시간 안에 표시되지 않으면, 전처리기는 상태 표에서 스트림을 삭제합니다.

Threat Defense 디바이스는 이 옵션을 무시하며, 대신 고급 액세스 컨트롤 **Threat Defense Service Policy(**위협 방어 서비스 정책**)**의 설정을 사용합니다. 자세한 내용은 서비스 정책 규칙 구성를 참조하십시오.

패킷 유형 성능 증대

활성화된 규칙에 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 TCP 트래픽을 무시하도록 전처리기를 설정합니다. 단, 소스 및 대상 포트가 모두 `any`로 설정된 UDP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 예외입니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다.

UDP 스트림 전처리 구성

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** **Transport/Network Layer Preprocessors(**전송/네트워크 계층 전처리기**)**의 **UDP Stream Configuration(UDP** 스트림 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **UDP Stream Configuration(UDP** 스트림 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** UDP 스트림 전처리 옵션, 38 페이지에 설명된 대로 옵션을 설정합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 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.하려면 관련 패킷 디코더 규칙(GID 116)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정 및 패킷 디코더, 20 페이지의 내용을 참조하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책