IAB(Intelligent Application Bypass)

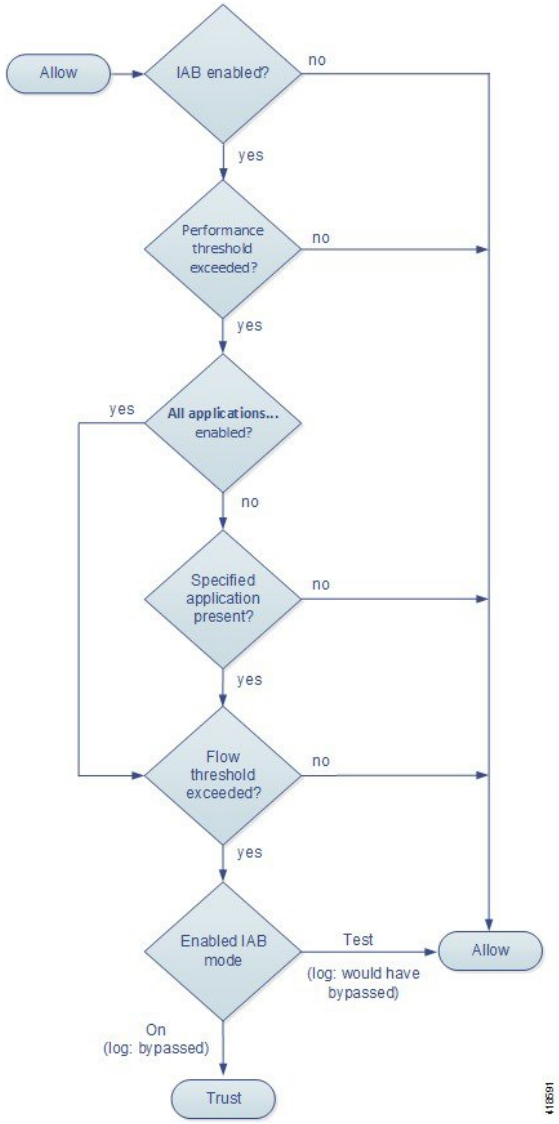
다음 주제에서는 Intelligent Application Bypass(IAB)를 사용하도록 액세스 제어 정책을 구성하는 방법을 설명합니다.

IAB 소개

IAB는 성능 및 플로우 임계값 초과 시 추가 검사 없이 네트워크를 통과하도록 신뢰하는 애플리케이션을 식별합니다. 예를 들어 야간 백업이 시스템 성능에 크게 영향을 주는 경우 초과 시에 백업 애플리케이션에서 생성하는 트래픽을 신뢰하는 임계값을 구성할 수 있습니다. 이 옵션에는 6.0.1.4 버전 또는 후속 6.0.1.x 패치가 필요합니다. 필요에 따라 애플리케이션 유형에 관계없이 검사 성능 임계값을 초과할 때 IAB가 플로우 바이패스 임계값을 초과하는 모든 트래픽을 신뢰하도록 IAB를 구성할 수 있습니다.

시스템은 트래픽을 심층 검사하기 전에 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업에서 허용하는 트래픽에 대해 IAB를 구현합니다. 테스트 모드를 적용하면 임계값 초과 여부를 확인할 수 있으며, 임계값이 초과되는 경우에는 IAB를 실제로 활성화했을 때(바이패스 모드) 바이패스되는 애플리케이션 플로우를 식별할 수 있습니다.

다음 그래픽에서는 IAB 관련 의사 결정 프로세스를 보여줍니다.



IAB 옵션

상태

IAB를 활성화하거나 비활성화합니다.

성능 샘플링 간격

IAB 성능 샘플링 검사 간의 시간(초)을 지정합니다. IAB 성능 샘플링 검사에서는 시스템이 IAB 성능 임계값과 비교할 시스템 성능 메트릭을 수집합니다. 값을 **0**으로 설정하면 IAB가 비활성화됩니다.

바이패스 가능한 애플리케이션 및 필터

이 기능은 함께 사용할 수 없는 두 가지 옵션을 제공합니다.

애플리케이션/필터
: 우회할 수 있는 애플리케이션 및 애플리케이션 집합(필터)을 지정할 수 있는 편집기를 제공합니다. 애플리케이션 조건(애플리케이션 컨트롤)의 내용을 참조하십시오.

알 수 없는 애플리케이션을 포함한 모든 애플리케이션
: 애플리케이션 유형에 관계없이 검사 성능 임계값을 초과할 때 플로우 바이패스 임계값을 초과하는 모든 트래픽을 신뢰합니다.

성능 및 플로우 임계값

적어도 하나의 검사 성능 임계값과 하나의 흐름 우회 임계값을 구성해야 합니다. 성능 임계값이 초과되면 시스템은 흐름 임계값을 검사하고 하나의 임계값이 초과된 경우, 지정된 트래픽을 신뢰합니다. 두 임계값을 모두 활성화한 경우, 그중 하나만 초과되어야 합니다.

검사 성능 임계값은 초과하는 경우 플로우 임계값 검사를 트리거하는 침입 검사 성능 제한을 제공합니다. IAB는 **0**으로 설정된 검사 성능 임계값을 사용하지 않습니다. 다음 검사 성능 임계값 중 하나 이상을 구성할 수 있습니다.

삭제율

: 고가의 침입 규칙, 파일 정책, 압축 해제 등으로 인해 발생하는 성능 오버로드 때문에 패킷이 삭제될 때 삭제되는 평균 패킷 수(총 패킷의 퍼센트)입니다. 침입 규칙 등의 일반 컨피그레이션으로 인해 삭제되는 패킷은 포함되지 않습니다. 1보다 큰 정수를 지정하는 경우 지정된 퍼센트만큼 패킷이 삭제되면 IAB가 활성화됩니다. 값을 **1**로 지정하는 경우, 퍼센트가 0~1 사이이면 IAB가 활성화됩니다. 즉, 삭제되는 패킷 수가 적더라도 IAB를 활성화할 수 있습니다.

프로세서 사용률

: 사용되는 프로세서 리소스의 평균 퍼센트입니다.

패키지 레이턴시

: 평균 패킷 레이턴시(마이크로초)입니다.

플로우 속도

: 초당 플로우 수로 측정된 시스템 프로세스가 이동하는 속도입니다. 이 옵션은 플로우 개수가 아닌 플로우 속도를 측정하도록 IAB를 구성합니다.

플로우 바이패스 임계값은 초과하는 경우 IAB가 우회 가능한 애플리케이션 트래픽을 신뢰(우회 모드)하도록 하거나 애플리케이션 트래픽을 추가로 검사(테스트 모드)할 수 있도록 하는 플로우 제한을 제공합니다. IAB는 **0**으로 설정된 플로우 바이패스 임계값을 사용하지 않습니다. 다음 흐름 우회 임계값 중 하나 이상을 구성할 수 있습니다.

플로우당 바이트

: 플로우가 포함할 수 있는 최대 킬로바이트 수입니다.

플로우당 패킷

: 플로우가 포함할 수 있는 최대 패킷 수입니다.

플로우 지속시간

플로우를 열어 둘 수 있는 최대 시간(초)입니다.

플로우 속도

최대 전송 속도(초당 킬로바이트)입니다.

인텔리전트 애플리케이션 우회에 대한 요구 사항 및 사전 조건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

Intelligent Application Bypass 구성

⚠

주의 모든 구축에 IAB가 필요한 것은 아니며 IAB가 필요한 구축에서는 제한된 방식으로 IAB를 사용합니다. 네트워크 트래픽(특히 애플리케이션 트래픽)과 시스템 성능(예측 가능한 성능 문제의 원인 포함)에 대해 철저하게 파악하고 있지 않다면 IAB를 활성화하지 마십시오. 바이패스 모드에서 IAB를 실행하기 전에 지정한 트래픽을 신뢰하는 경우 위험이 발생하지 않는지를 확인하십시오.

시작하기 전에

클래식 디바이스의 경우에는 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 **Intelligent Application Bypass Settings(Intelligent Application Bypass** 구성**)** 옆의 수정( )을 클릭합니다.

보기 아이콘(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** IAB 옵션을 구성합니다.

- State(상태) - IAB **Off(**끄기**)** 또는 **On(**켜기**)**을 선택하거나 **Test(**테스트**)** 모드에서 IAB를 활성화합니다.
- Performance Sample Interval(성능 샘플링 간격) - IAB 성능 샘플링 검사 간의 시간(초)을 입력합니다. IAB를 활성화하는 경우에는 테스트 모드에서도 0이 아닌 값을 입력합니다. **0**을 입력하면 IAB가 비활성화됩니다.
- Bypassable Applications and Filters(바이패스 가능한 애플리케이션 및 필터) - 다음 중에서 선택합니다.
  - 우회한 애플리케이션 및 필터 수를 클릭하고 트래픽을 우회하려는 애플리케이션을 지정합니다. 애플리케이션 조건 및 필터 구성 참조.
  - **All applications including unidentified applications(**알 수 없는 애플리케이션을 포함한 모든 애플리케이션**)**를 클릭합니다. 그러면 애플리케이션 유형에 관계없이 검사 성능 임계값을 초과할 때 IAB가 플로우 바이패스 임계값을 초과하는 모든 트래픽을 신뢰합니다.
- Inspection Performance Thresholds(검사 성능 임계값) - **Configure(**구성**)**를 클릭하고 임계값을 하나 이상 입력합니다.
- Flow Bypass Thresholds(플로우 바이패스 임계값) - **Configure(**구성**)**를 클릭하고 임계값을 하나 이상 입력합니다.

검사 성능 임계값과 플로우 바이패스 임계값을 각각 하나 이상 지정해야 합니다. 이 두 임계값을 모두 초과해야 IAB가 플로우를 신뢰합니다. 각 유형의 임계값을 여러 개 입력하는 경우에는 각 유형의 임계값을 하나만 초과하면 됩니다. 자세한 정보는 IAB 옵션, 2 페이지의 내용을 참고하십시오.

단계 **3** **OK(**확인**)**를 클릭하여 IAB 설정을 저장합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 일부 패킷은 애플리케이션이 탐지되기 전에 통과하도록 허용해야 하므로 해당 패킷을 검사하도록 시스템을 설정해야 합니다.

  트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례 및 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정를 참조하십시오.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

IAB 로깅 및 분석

IAB는 연결 로깅을 활성화했는지 여부에 관계없이 실제로 바이패스된 플로우와 IAB 활성화 시 바이패스되었을 플로우를 로깅하는 연결 종료 이벤트를 강제로 생성합니다. 연결 이벤트는 바이패스 모드에서 바이패스된 플로우와 테스트 모드에서 IAB 활성화 시 바이패스되었을 플로우를 나타냅니다. 연결 이벤트를 기반으로 하는 맞춤형 대시보드 위젯과 보고서에 바이패스된 플로우와 바이패스되었을 플로우의 장기 통계를 표시할 수 있습니다.

IAB 연결 이벤트

작업

Reason(이유**)**에 `Intelligent App Bypass`가 포함된 경우:

`Allow(`허용**`)` -**

적용된 IAB 구성이 테스트 모드였으며 **Application Protocol(**애플리케이션 프로토콜**)**로 지정된 애플리케이션의 트래픽이 계속 검사할 수 있는 상태임을 나타냅니다.

`Trust(`신뢰**`)` -**

적용된 IAB 구성이 우회 모드였으며 **Application Protocol(**애플리케이션 프로토콜**)**로 지정된 애플리케이션의 트래픽이 추가 검사 없이 네트워크를 통과하도록 신뢰되었음을 나타냅니다.

이유

`Intelligent App Bypass`는 IAB가 바이패스 또는 테스트 모드에서 이벤트를 트리거했음을 나타냅니다.

애플리케이션 프로토콜

이 필드에는 이벤트를 트리거한 애플리케이션 프로토콜이 표시됩니다.

예

아래의 잘린 그래픽에서는 일부 필드가 생략되었습니다. 이 그래픽에는 두 개별 액세스 제어 정책의 각기 다른 IAB 설정에서 생성되는 연결 이벤트 2개에 대한 **Action(**작업**)**, **Reason(**이유**)** 및 **Application Protocol(**애플리케이션 프로토콜**)** 필드가 나와 있습니다.

첫 번째 이벤트에서 `Trust(신뢰)` 작업은 IAB가 바이패스 모드에서 활성화되었으며 Bonjour 프로토콜 트래픽이 추가 검사 없이 통과하도록 신뢰되었음을 나타냅니다.

두 번째 이벤트에서 `Allow(허용)` 작업은 IAB가 테스트 모드에서 활성화되었으므로 Ubuntu Update Manager 트래픽이 추가로 검사되지만 IAB가 바이패스 모드였다면 바이패스되었을 것임을 나타냅니다.

Action	Reason	Application Protocol
Trust	Intelligent App Bypass	Bonjour
Allow	Intelligent App Bypass	Ubuntu Update Manager

404433

예

아래의 잘린 그래픽에서는 일부 필드가 생략되었습니다. 두 번째 이벤트의 플로우는 둘 다 바이패스되었으며(**Action(**작업**)**: `Trust(신뢰)`, **Reason(**이유**)**: `Intelligent App Bypass`) 침입 규칙을 통해 검사되었습니다(**Reason(**이유**)**: `Intrusion Monitor(침입 모니터링)`). 이유가 `Intrusion Monitor(침입 모니터링)`인 경우 **Generate Events(**이벤트 생성**)**로 설정된 침입 규칙이 탐지되었지만 연결 중에 익스플로잇이 차단되지는 않았음을 나타냅니다. 애플리케이션이 탐지되기 전에 침입 규칙이 탐지된 경우를 예로 들 수 있습니다. 애플리케이션이 탐지되고 나면 IAB는 해당 애플리케이션을 바이패스 가능한 것으로 인식하고 플로우를 신뢰합니다.

Last Packet	Action	Reason	Application Protocol
2015-06-12 10:53:09	Trust	Intelligent App Bypass	Skype Probe
2015-06-12 10:53:08	Trust	Intelligent App Bypass, Intrusion Monitor	HTTP

404541

IAB 맞춤형 대시보드 위젯

연결 이벤트에 따라 장기 IAB 통계를 표시할 맞춤형 분석 대시보드 위젯을 생성할 수 있습니다. 위젯을 생성할 때는 다음 사항을 지정합니다.

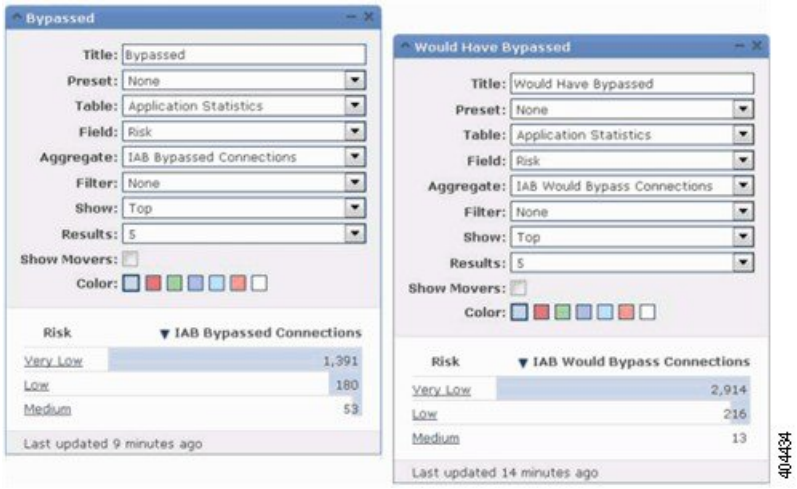
- **Preset(**사전 설정**)**: `None(없음)`
- **Table(**테이블**)**: `Application Statistics(애플리케이션 통계)`
- **Field(**필드**)**: any(모두)
- **Aggregate(**집계**)**: 다음 중 하나
  - `IAB에서 바이패스된 연결 수`
  - `IAB에서 바이패스되는 연결 수`
- **Filter(**필터**)**: any(모두)

예

아래에는 맞춤형 분석 대시보드 위젯의 예시와 해당 설명이 나와 있습니다.

- *Bypassed(*바이패스됨*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 바이패스 모드로 활성화되었기 때문에 바이패스된 애플리케이션 트래픽에 대한 통계를 보여줍니다.

- *Would Have Bypassed(*바이패스되었을 것임*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 테스트 모드로 활성화되었기 때문에 실제로 IAB가 활성화되면 바이패스되었을 애플리케이션 트래픽에 대한 통계를 보여줍니다. .



IAB 맞춤형 보고서

연결 이벤트에 따라 장기 IAB 통계를 표시할 맞춤형 보고서를 생성할 수 있습니다. 보고서를 생성할 때는 다음 사항을 지정합니다.

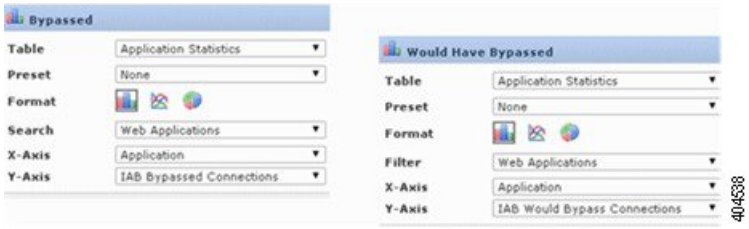
- **Table(**테이블**)**: `Application Statistics(애플리케이션 통계)`
- **Preset(**사전 설정**)**: `None(없음)`
- **Filter(**필터**)**: any(모두)
- **X-Axis(X**축**)**: any(모두)
- **Y-Axis(Y**축**)**: 다음 중 하나
  - `IAB에서 바이패스된 연결 수`
  - `IAB에서 바이패스되는 연결 수`

예

다음 그래픽은 간략하게 표시된 두 보고서 예시를 보여줍니다.

- *Bypassed(*바이패스됨*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 바이패스 모드로 활성화되었기 때문에 바이패스된 애플리케이션 트래픽에 대한 통계를 보여줍니다.
- *Would Have Bypassed(*바이패스되었을 것임*)* 예시에서는 애플리케이션이 바이패스 가능한 것으로 지정되었으며 구축된 액세스 제어 정책에서 IAB가 테스트 모드로 활성화되

었기 때문에 실제로 IAB가 활성화되면 바이패스되었을 애플리케이션 트래픽에 대한 통계를 보여줍니다.



관련 항목

- 연결 및 보안 인텔리전스 이벤트 필드
- 맞춤형 분석 위젯
- 대시보드에 위젯 추가
- 보고서 템플릿