위협 탐지

Cisco의 포트스캔 탐지기는 모든 유형의 트래픽에서 포트스캔 활동을 탐지하고 방지하여 최종 공격으로부터 네트워크를 보호하도록 설계된 위협 탐지 메커니즘입니다. 포트스캔 트래픽은 허용된 트래픽과 거부된 트래픽 모두에서 효율적으로 탐지할 수 있습니다.

포트스캔은 공격에 앞서 공격자가 종종 사용하는 네트워크 정찰의 형태입니다. 포트스캔에서 공격자는 호스트가 지원하는 네트워크 프로토콜 또는 서비스의 유형을 확인하고 특수하게 조작된 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.

참고 액세스 제어 정책의 포트스캔 탐지 및 방지 기능은 Snort 3 디바이스에서만 management center 7.2부터 지원됩니다. Snort에서 검사하는 트래픽에만 위협 탐지가 가능합니다. 위협 방어 디바이스 자체로 전송된 트래픽에 대한 위협 탐지는 고려되지 않습니다.

포트스캔 탐지 및 방지

탐지 유형

다음은 호스트가 탐지하는 것을 차단할 수 있는 포트스캔 활동 유형입니다.

- **Regular portscan(**일반 포트스캔**)** - 공격자가 단일 대상 호스트에서 여러 포트를 스캔하기 위해 하나의 호스트를 사용하는 일대일 포트스캔입니다. 이 옵션은 TCP, UDP 및 IP 포트스캔을 탐지합니다.

- **Decoy portscan(Decoy** 포트스캔**)** - 공격자가 실제 스캐닝 IP 주소와 스푸핑된 소스 IP 주소를 혼합하는 일대일 포트스캔입니다. Decoy 포트스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.
- **Distributed portscan(**분산형 포트스캔**)** - 여러 호스트가 개방형 포트를 위해 단일 호스트를 쿼리하는 다대일 포트스캔입니다. 이는 여러 호스트에서 제공되는 모든 요청이 합법적으로 보일 수 있으므로 포트스캔 탐지를 회피하는 데 사용됩니다. 분산형 포트스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.
- **Port sweep(**포트 스윕**)** - 공격자가 하나 또는 여러 호스트를 사용하여 여러 대상 호스트에서 단일 포트를 스캔하는 일대다 포트 스윕입니다. 이는 대개 새로운 익스플로잇에서 발생하며 공격자는 특정 서비스를 찾고 있습니다. 이 옵션은 TCP, UDP, ICMP 및 IP 포트 스윕을 탐지합니다.

참고 일반, Decoy 및 분산형 포트스캔은 일반 포트스캔 활동으로 분류되지 않으며 알림을 받습니다.

Traffic Selection(트래픽 선택**)**

- **Permitted(**허용됨**)**, **Denied(**거부됨**)** 또는 **All(**모두**)** 트래픽에 대해 포트스캔 탐지를 선택할 수 있습니다. 기본적으로 포트스캔 탐지는 선택한 범주의 모든 트래픽에 대해 발생합니다.
- 포트스캔 활동을 모니터링할 네트워크를 지정할 수 있습니다. 모니터링되는 네트워크 내에서 특정 호스트가 스캐너로 식별되는 것을 제외할 수 있습니다.
- 대상 호스트로 향하는 모든 트래픽을 포트스캔 탐지에서 제외할 수도 있습니다.
- 포트스캔 탐지는 IPv4 및 IPv6 트래픽 모두에 대해 지원됩니다.

탐지 구성

탐지 구성 옵션은 다음과 같습니다.

- 구성 옵션:
  - Protocol types(프로토콜 유형): TCP, UDP, IP, ICMP
  - 포트 수(Port count): TCP 및 UDP 기반 스캔을 위해 액세스되는 포트 수
  - Host count(호스트 수): TCP, UDP 및 ICMP 기반 스캔을 위해 액세스되는 호스트 수
  - Protocol count(프로토콜 수): IP 프로토콜 스캔에 사용되는 프로토콜 수
  - Interval(간격): 시간 간격
- Predefined sensitivity levels(사전 정의된 민감도 레벨) - 다음 민감도 레벨을 사용하여 포트스캔 탐지를 조정할 수 있습니다.
  - Low(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.

- Medium(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.

  기본적으로 민감도 레벨은 **Medium(**중간**)**으로 설정됩니다.

  이 레벨은 포트스캔 탐지에 좀 더 긴 시간 창을 사용합니다.

- High(높음) - 정해진 기간을 기반으로 포트스캔을 탐지합니다. 즉, 시간 기반 포트스캔을 탐지할 수 있습니다. 이 레벨은 포트스캔 탐지에 훨씬 긴 시간 창을 사용합니다.

- Custom(사용자 지정) - 민감도 레벨을 사용자 지정하려는 경우 사용합니다. 기존의 사전 구성된 민감도 레벨을 편집하는 경우 **Custom(**사용자 지정**)** 옵션이 자동으로 선택됩니다.

- 임계값을 세부적으로 조정할 수 있고, 다양한 스캔 유형을 활성화하거나 비활성화할 수도 있습니다.

방지 구성

방지 구성에는 다음과 같은 옵션이 있습니다.

- 포트스캔 활동을 수행하는 것으로 식별된 호스트를 차단할 수 있습니다.
- 기간 만료 후 호스트의 차단을 자동으로 해제하는 기간 기반 차단을 사용할 수 있습니다.
- 호스트가 포트스캔 활동으로 인해 차단되는 것을 제외할 수 있습니다.

포트스캔 탐지 및 방지 구성, 3 페이지 항목을 참고하십시오.

포트스캔 탐지 및 방지 구성

포트스캔을 탐지하거나 방지하도록 구성할 수 있습니다. 기본적으로 포트스캔 탐지는 허용되는 트래픽에서만 이루어집니다.

시작하기 전에

액세스 제어 정책 편집기에서 포트스캔 탐지 및 방지를 구성하려면 다음 사전 요건을 충족해야 합니다.

- Management Center 및 매니지드 디바이스에서 7.2.0 이상을 실행해야 합니다.
- Snort 3을 활성화해야 합니다.

참고 Snort 3에서 Snort 2로 디바이스를 전환하면 포트스캔이 비활성화됩니다. 그러나 NAP 및 침입 정책을 사용하여 Snort 2를 사용하는 디바이스에서 포트스캔을 구성할 수 있습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 클릭합니다. 그런 다음 **Threat Detection(**위협 탐지**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **2** **Threat Detection(**위협 탐지**)** 창에서 **Portscan mode(**포트스캔 모드**)**로 **Detection(**탐지**)** 또는 **Prevention(**방지**)**를 선택할 수 있습니다.

단계 **3** **Detection(**탐지**)**를 선택하는 경우:

1. **Traffic Selection(**트래픽 선택**)** 탭에는 **Permitted(**허용됨**)**, **Denied(**거부됨**)** 또는 **All(**모두**)** 트래픽에 대한 포트스캔 탐지를 선택하는 옵션이 있습니다.
2. **Monitor(**모니터링**)**, **Ignore Scanner(**스캐너 무시**)** 및 **Ignore Target(**대상 무시**)** 필드에서 포트스캔 탐지를 고려(모니터링)할 IP 또는 네트워크, 공격자로 무시할 IP 또는 네트워크, 대상 호스트로 무시할 IP 또는 네트워크를 선택할 수 있습니다.

   참고 FQDN, 와일드카드 마스크, any, any-ipv4 및 any-ipv6 네트워크 개체는 포트스캔 구성에 지원되지 않습니다. 이러한 개체는 **Monitor(**모니터링**)**, **Ignore Scanner(**스캐너 무시**)**, **Ignore Target(**대상 무시**)** 및 **Exclude(**제외**)** 필드에 표시되지 않습니다.

3. **Configuration(**구성**)** 탭에서 사전 구성된 민감도 레벨을 **Low(**낮음**)**, **Medium(**중간**)**, **High(**높음**)** 또는 **Custom(**사용자 지정**)**으로 선택하여 포트스캔 탐지를 조정합니다. 민감도 레벨을 사용자 지정하려면 **Custom(**사용자 지정**)** 옵션을 선택합니다.
4. 다양한 프로토콜 유형(TCP, UDP, IP, ICMP)에서 액세스되는 호스트 수, 액세스되는 포트 수, 사용되는 프로토콜 수(IP 프로토콜의 경우), 간격을 설정할 수 있습니다.

단계 **4** **Prevention(**방지**)** 포트스캔 모드를 선택하여 호스트가 네트워크를 추가로 스캔하거나 공격을 호스팅하지 못하도록 차단할 수 있습니다. **Prevention(**방지**)** 탭의 **Exclude(**제외**)**에서 IP 또는 네트워크가 차단에서 제외되도록 선택하고 호스트를 차단할 **Duration(**기간**)**을 설정할 수 있습니다.

단계 **5** 포트스캔 설정을 기본(비활성화) 상태로 되돌리려면 **Revert to Defaults(**기본값으로 되돌리기**)** 옵션을 클릭합니다.

단계 **6** **OK(**확인**)**를 클릭하여 포트스캔 탐지 및 방지 설정을 저장합니다.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

참고 포트스캔 구성 변경 사항은 AC 정책 감사 로그 보고서의 일부로 제공됩니다.

다음에 수행할 작업

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

낮은 민감도에서 향상된 탐지

낮은 민감도 수준에서 TCP, UDP 및 ICMP 초기 패킷에 대한 부정적인 응답을 추적할 수 있습니다. 실패한 연결 수가 거부 임계값(예: 낮은 민감도에서 10%)보다 크고 포트/IP 프로토콜 수가 구성된 임계값보다 많은 경우에만 알림이 트리거됩니다. 이는 오탐을 완화합니다.

허용된 트래픽과 차단된 트래픽이 혼합된 경우, 허용된 트래픽과 차단된 트래픽의 차이를 기반으로 거부 포트 또는 호스트 수가 계산됩니다. 차단된 트래픽만 있는 경우에는 거부 임계값이 고려되지 않습니다.

주의 위협 방어가 인라인 설정 모드로 구성된 경우 이 솔루션은 UDP 및 ICMP 연결에서 작동하지 않습니다.

예

포트스캔이 낮은 민감도의 위협 방어에서 활성화된다고 가정합니다.

구성된 포트 수 임계값 = 120

계산된 거부 수 임계값 = 120의 10% = 12

공격자가 대상의 131개 포트를 사용하여 연결을 개시하며, 대상이 모든 개시를 긍정적으로 확인합니다. 포트 수 131개는 임계값보다 크지만 부정적 확인이 없으므로 알림이 트리거되지 않습니다.

공격자가 대상의 131개 포트를 사용하여 연결을 개시하며, 대상이 121개의 개시를 긍정적으로 확인하고 10개의 개시를 부정적으로 확인합니다.

포트 수 131개는 임계값보다 크지만 거부 포트 수 10개는 거부 임계값보다 작으므로 알림이 트리거되지 않습니다.

공격자가 대상의 134개 포트를 사용하여 연결을 개시하며, 대상이 121개의 개시를 긍정적으로 확인하고 13개의 개시를 부정적으로 확인합니다. 포트 수 134개는 임계값보다 크고 거부 포트 수 13개도 거부 임계값보다 큽니다. 따라서 이 경우 알림이 트리거됩니다.

알림 - 포트스캔 활동

포트스캔을 구성하는 경우 IPS 정책 또는 이벤트의 존재나 구성에 상관없이 포트스캔 관련 침입 정책 이벤트가 생성됩니다.

포트스캔 활동은 기존 포트스캔 관련 IPS 이벤트를 통해 알림이 전송됩니다. GID(Generator ID)가 122이고 SID(Snort ID)가 1~27인 IPS 이벤트가 생성됩니다. 이러한 이벤트의 경우 *(port_scan)* 문자열이 이벤트 메시지 앞에 추가됩니다.

management center에서 이러한 이벤트를 보려면 **Analysis(**분석**)** > **Intrusion(**침입**)** > **Events(**이벤트**)**로 이동합니다.

NAP 정책에서 포트스캔 업그레이드

7.2.0 이상을 실행하는 디바이스에서는 Snort 3 NAP(네트워크 분석 정책) 기반 포트스캔 기능이 지원되지 않습니다.

7.2.0 이상 버전을 실행하는 Snort 3 디바이스의 경우, 액세스 제어 정책(Advanced settings(고급 설정) 탭)을 사용하여 포트스캔을 구성해야 합니다.

7.2.0 이상 Snort 3 디바이스로 업그레이드한 경우 포트스캔 구성 설정이 NAP 정책 대신 액세스 제어 정책 포트스캔 설정에서 선택 및 구축되므로, NAP 포트스캔 구성을 AC 정책 포트스캔으로 마이그레이션하지 않은 경우 디바이스에서 다음 구축 시 포트스캔 구성이 손실됩니다.

다음 표에는 Snort 3 또는 Snort 2 엔진을 실행하는 7.2.0 이상 버전 및 7.1.0 이하 버전에 적용할 수 있는 포트스캔 구성이 나와 있습니다.

FMC	**FTD**	포트스캔 구성
FMC 7.0 또는 7.1	Snort 2 디바이스	Snort 2 NAP 정책의 구성을 적용할 수 있습니다.
	Snort 3 디바이스	Snort 3 NAP 정책의 구성을 적용할 수 있습니다.
FMC 7.2.0	Snort 2 디바이스	Snort 2 NAP 정책의 구성을 적용할 수 있습니다.
	Snort 3 디바이스(7.1.0 이하)	Snort 3 NAP 정책의 구성을 적용할 수 있습니다.
	Snort 3 디바이스(7.2.0 이상)	액세스 제어 정책의 구성을 적용할 수 있습니다.

포트스캔 액세스 제어 정책에 대한 기능 지원

포트스캔을 포함한 액세스 제어 정책에는 다음 기능이 지원됩니다.

- 감사 로그 및 델타 미리보기 - 포트스캔 정보는 AC 정책 감사 로그 및 Depoyment Preview(구축 미리보기)에서 제공됩니다.
- 가져오기 및 내보내기 – 포트스캔 구성이 포함된 AC 정책을 가져오거나 내보낼 수 있습니다.
- 도메인 – 글로벌 및 리프 도메인의 AC 정책에 포트스캔을 구성할 수 있습니다.
- **PDF** 보고서 생성 – AC 정책 보고서에는 구성된 포트스캔 설정도 포함됩니다.
- 롤백 – 포트스캔 구성을 포함하는 구성의 구축된 버전으로 롤백할 수 있습니다.