침입 이벤트에 대한 외부 알림

다음 주제에서는 침입 이벤트에 대한 외부 경고 설정 방법을 설명합니다.

침입 이벤트에 대한 외부 알림 정보

외부 침입 이벤트 알림으로 중요 시스템 모니터링을 지원할 수 있습니다.

- SNMP - 침입 정책별로 설정되며 매니지드 디바이스에서 전송됩니다. 침입 규칙별로 SNMP 알림을 활성화할 수 있습니다.
- Syslog(시스템 로그) - 침입 정책별로 설정되며 매니지드 디바이스에서 전송됩니다. 침입 규칙에서 시스템 로그 알림을 설정하는 경우, 정책의 모든 규칙에 대해 알림을 설정하게 됩니다.
- Email(이메일) - 모든 침입 정책에서 설정되며 Firepower Management Center에서 전송합니다. 침입 규칙별로 이메일 알림을 활성화하고, 알림의 길이와 빈도를 제한할 수 있습니다.

침입 이벤트 억제 또는 임계값 설정을 설정하는 경우, 시스템은 규칙이 트리거될 때마다 침입 규칙을 생성하지는 않는다는 점을(그리고 그에 따라 알림을 전송하지 않을 수도 있음을) 유의하십시오.

다중 도메인 구축의 경우, 모든 도메인에서 외부 알림을 설정할 수 있습니다. 상위 도메인의 경우, 시스템은 하위 도메인의 침입 이벤트에 대한 알림을 생성합니다.

참고 또한 Firepower Management Center은(는) SNMP, 시스템 로그, 이메일 알림 응답을 사용하여 다양한 유형의 외부 알림을 전송합니다(Firepower Management Center 알림 응답 참조). 시스템은 알림 응답을 이용해 개별 침입 이벤트를 바탕으로 알림을 보내지는 않습니다.

관련 항목

침입 정책의 침입 이벤트 알림 필터

침입 이벤트 외부 알림 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

침입 이벤트 외부 알림 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 이벤트에 대한 **SNMP** 알림 설정

침입 정책에서 외부 SNMP 알림을 활성화하면, 개별 규칙을 설정해 트리거 시 SNMP 알림을 보낼 수 있습니다. 이러한 알림은 매니지드 디바이스에서 전송됩니다.

프로시저

단계 **1** 침입 정책 편집기의 탐색창에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **SNMP Alerting(SNMP** 알림**)**이 **Enabled(**활성화**)**인지 확인하고 **Edit(**편집**)**를 클릭합니다.
페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다.

단계 **3** **SNMP** 버전을 클릭하고 침입 SNMP 알림 옵션, 3 페이지에 설명된 대로 설정 옵션을 지정합니다.

단계 **4** 탐색 창에서 **Rules(**규칙**)**를 클릭합니다.

단계 **5** 규칙 창에서 SNMP 알림을 설정할 규칙을 선택하고 **Alerting(**알림**)** > **Add SNMP Alert(SNMP** 알림 추가**)**을(를) 선택합니다.

단계 **6** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 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

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

침입 **SNMP** 알림 옵션

네트워크 관리 시스템에 Firepower Management Center의 MIB(Management Information Base) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

SNMP v2 옵션

옵션	설명
트랩 유형	경고에 나타나는 IP 주소를 사용할 트랩 유형입니다. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(**이진으로**)**을(를) 선택합니다. 그렇지 않은 경우에는 **as String(**문자열로**)**을 선택합니다. 예를 들어 HP OpenView는 **as String(**문자열로**)** 옵션이 필요합니다.
트랩 서버	SNMP 트랩 알림을 받을 서버입니다. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
커뮤니티 문자열	커뮤니티 이름입니다.

SNMP v3 옵션

매니지드 디바이스는 SNMPv3 알림을 Engine ID 값으로 인코딩합니다. 알림을 디코딩할 때 SNMP 서버는 이 값을 요구합니다. 이 값은 전송하는 디바이스의 인터페이스 IP 주소의 16진수 버전으로, "01"이 붙습니다.

예를 들어 SNMP 알림을 전송하는 디바이스의 관리 인터페이스 IP 주소가 172.16.1.50인 경우, Engine ID 값은 0xAC10013201입니다.

옵션	설명
트랩 유형	경고에 나타나는 IP 주소를 사용할 트랩 유형입니다. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(**이진으로**)**을(를) 선택합니다. 그렇지 않은 경우에는 **as String(**문자열로**)**을 선택합니다. 예를 들어 HP OpenView는 **as String(**문자열로**)** 옵션이 필요합니다.
트랩 서버	SNMP 트랩 알림을 받을 서버입니다. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
인증 비밀번호	인증을 위해 필요한 비밀번호입니다. SNMP v3은 이 비밀번호를 암호화하기 위해 메시지 다이제스트 5(MD5) 해시 함수 또는 보안 해시 알고리즘(SHA) 해시 함수를 사용하며, 이는 구성에 따른 것입니다. 인증 비밀번호를 지정한 경우, 인증이 활성화됩니다.
개인 비밀번호	프라이버시를 위한 SNMP 키입니다. SNMP v3은 이 비밀번호를 암호화하기 위해 데이터 암호화 표준(DES) 블록 암호를 사용합니다. SNMP v3 비밀번호를 입력할 때, 해당 비밀번호는 초기 구성 중에 일반 텍스트로 표시되지만 암호화된 형식으로 저장됩니다. 개인 비밀번호를 지정한 경우 프라이버시가 활성화되며, 인증 비밀번호도 반드시 지정해야 합니다.
User Name(사용자 이름)	SNMP 사용자 이름입니다.

침입 이벤트를 위한 시스템 로그 알림 설정

침입 정책에서 시스템 로그 알림을 활성화하면, 시스템은 모든 침입 이벤트를 매니지드 디바이스 자체 또는 외부 호스트의 시스템 로그로 전송합니다. 외부 호스트를 지정하는 경우, 시스템 로그 알림은 매니지드 디바이스에서 전송됩니다.

프로시저

단계 **1** 침입 정책 편집기의 탐색창에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **Syslog Alerting(**시스템 로그 알림**)**이 **Enabled(**활성화**)**인지 확인하고 **Edit(**편집**)**를 클릭합니다.
페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. **Syslog Alerting(**시스템 로그**)** 알림 페이지가 **Advanced Settings(**고급 설정**)**에 추가됩니다.

단계 **3** 시스템 로그 알림을 전송할 **Logging Hosts(**기록 호스트**)**의 IP 주소를 입력합니다.

Logging Hosts(기록 호스트**)** 필드를 입력하지 않는 경우 기록 호스트 상세정보는 연결된 Access Control Policy(액세스 컨트롤 정책)의 Logging(기록)에서 가져옵니다.

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 **4** 침입 시스템 로그 알림에 대한 시설 및 Severities(심각도), 5 페이지에 설명된 대로 **Facility(**시설**)** 및 **Severity(**심각도**)**을(를) 선택합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 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

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

침입 시스템 로그 알림에 대한 시설 및 **Severities(**심각도**)**

매니지드 디바이스는 기록 호스트가 알림을 분류할 수 있도록, 특정 시설 및 **Severity(**심각도**)**를 사용하여 침입 이벤트를 시스템 로그 알림으로 전송할 수 있습니다. 시설은 이를 생성한 하위 시스템을 지정합니다. 이러한 시설 및 **Severity(**심각도**)** 값은 실제 시스템 로그 메시지에는 표시되지 않습니다.

환경에 맞는 합리적인 값을 선택합니다. 로컬 설정 파일(UNIX 기반 기록 호스트에서의 syslog.conf 등)은 어떤 시설이 어떤 로그 파일에 저장되는지를 나타내기도 합니다.

시스템 로그 알림 시설

기능	설명
AUTH	보안 및 인증과 관련된 메시지입니다.
AUTHPRIV	보안 및 인증과 관련된 제한적 액세스 메시지입니다. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다.
CRON	클록 데몬에 의해 생성된 메시지입니다.
DAEMON	시스템 데몬에서 생성된 메시지입니다.
FTP	FTP 데몬에 의해 생성된 메시지입니다.
KERN	커널에 의해 생성된 메시지입니다. 여러 시스템에서 이 메시지가 나타나면 콘솔에 인쇄됩니다.
LOCAL0-LOCAL7	내부 프로세스에 의해 생성된 메시지입니다.
LPR	인쇄 하위 시스템에 의해 생성된 메시지입니다.

기능	설명
MAIL	메일 시스템에 의해 생성된 메시지입니다.
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지입니다.
SYSLOG	syslog 데몬에 의해 생성된 메시지입니다.
USER	사용자 레벨 프로세스에 의해 생성된 메시지입니다.
UUCP	UUCP 하위 시스템에 의해 생성된 메시지입니다.

시스템 로그 알림 심각도

레벨	설명
EMERG	모든 사용자에게 브로드캐스팅되는 공황 상태
ALERT	즉시 수정되어야 하는 상태
CRIT	심각한 상태
ERR	오류 상태
WARNING	경고 메시지
NOTICE	오류 상태는 아니지만 주의 필요
INFO	정보를 제공하는 메시지
DEBUG	디버그 정보를 포함하는 메시지

침입 이벤트에 대한 이메일 알림 설정

침입 이메일 알림을 활성화한 경우, 시스템은 침입을 매니지드 디바이스가 탐지했는지 침입 정책이 탐지했지와는 상관없이, 침입 이벤트 생성 시 이메일을 전송할 수 있습니다. 이러한 알림은 Firepower Management Center에서 전송됩니다.

시작하기 전에

- 이메일 알림을 받을 메일 호스트 설정합니다(메일 릴레이 호스트 및 알림 주소 구성 참조).
- Firepower Management Center이(가) 자체 IP 주소를 역확인할 수 있는지 확인합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Intrusion Email(**침입 이메일**)**을 클릭합니다.

단계 **3** 알림을 생성할 침입 규칙 또는 규칙 그룹을 포함한, 알림 옵션을 침입 이메일 알림 옵션, 7 페이지에 설명된 대로 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

침입 이메일 알림 옵션

On/Off(켜기/끄기**)**

침입 이메일 알림을 활성화 또는 비활성화합니다.

참고 활성화하면 개별 규칙을 선택하기 전에는 모든 규칙에 대한 알림이 활성화됩니다.

From/To Addresses(발신자/수신자 주소**)**

이메일 발신자 및 수신자입니다. 쉼표로 구분된 수신자 목록을 지정할 수 있습니다s.

최대 알림 및 빈도

Firepower Management Center이(가) 시간 간격(**Frequency(**빈도**)**)마다 전송할 이메일 알림의 최대 수(**Max Alerts(**최대 알림**)**)입니다.

알림 병합

같은 소스 IP와 규칙 ID를 이용하는 알림을 그룹화하여 전송하는 알림 수를 줄입니다.

요약 출력

텍스트 제한 디바이스에 적합한 짧은 알림을 활성화합니다. 짧은 알림은 다음 정보를 포함합니다.

- 타임스탬프
- 프로토콜
- 소스 및 목적지 IP와 포트
- Message
- 동일한 소스 IP에 대해 생성되는 침입 이벤트의 수

예: `2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: 알 수 없는 Datagram 디코딩 문제! (116:108)`

Summary Output(요약 출력**)**을 활성화하는 경우에는 **Coalesce Alerts(**알림 병합**)** 활성화도 고려해보십시오. 텍스트 메시지 제한 초과 예방을 위해 **Max Alerts(**최대 알림**)**를 낮춰야 할 수도 있습니다.

표준 시간대

알림 타임스탬프의 시간대입니다.

특정 규칙 설정에 관한 이메일 알림

이메일 알림을 설정할 규칙을 선택할 수 있습니다.