알림 응답을 사용한 외부 알림

다음 주제에서는 알림 응답을 사용하여 외부 이벤트 알림을 Secure Firewall Management Center에서 전송하는 방법을 설명합니다.

- Secure Firewall Management Center 알림 응답, 1 페이지
- 알림 응답 요구 사항 및 사전 요건, 2 페이지
- SNMP 알림 응답 생성, 3 페이지
- 시스템 로그 알림 응답 생성, 5 페이지
- 이메일 알림 응답 생성, 7 페이지
- 영향 플래그 알림 설정, 8 페이지
- 검색 이벤트 알림 설정, 9 페이지
- 악성코드 대응 알림 설정, 9 페이지

Secure Firewall Management Center 알림 응답

SNMP, 시스템 로그 또는 이메일을 통한 외부 이벤트 알림으로 중요 시스템 모니터링을 지원할 수 있습니다. Secure Firewall Management Center은(는) 설정 가능한 알림 응답을 이용해 외부 서버와 상호 작용합니다. 알림 응답은 이메일, SNMP 또는 시스템 로그 서버와의 연결을 나타나는 설정입니다. 응답이라고 부르는데, 이들을 이용해 Firepower가 탐지한 이벤트에 대한 응답으로 알림을 보낼 수 있기 때문입니다. 여러 알림 응답을 설정해 다양한 유형의 알림을 다양한 모니터링 서버 또는 사람에게 전송할 수 있습니다.

참고 디바이스와 Firepower 버전에 따라, 알림 응답이 시스템 로그 메시지를 전송하는 최상의 방법이 아닐 수도 있습니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드 및 보안 이벤트 시스템 로그 메시지 구성 모범 사례의 시스템 로그 정보 장을 참조하십시오. .

참고 알림 응답을 사용하는 알림은 Secure Firewall Management Center(으)로 전송합니다. 알림 응답을 사용하지 않는 침입 이메일 알림도 Secure Firewall Management Center(으)로 전송합니다. 반면 개별 침입 규칙 트리거링에 기반을 두는 SNMP와 시스템 로그 알림은 매니지드 디바이스가 직접 전송합니다. 자세한 내용은 침입 이벤트에 대한 외부 알림을 참조하십시오.

대부분의 경우 외부 알림에 있는 정보는 데이터베이스에 기록한 연결된 이벤트에 있는 정보와 동일합니다. 하지만 상관관계 규칙이 연결 추적기를 포함하는 상관관계 이벤트 알림의 경우, 수신하는 정보는 기본 이벤트 유형에 상관없이 트래픽 프로파일 변경에 대한 알림에 대한 정보와 동일합니다.

Alerts(알림) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**)에서 알림 응답을 생성하고 관리합니다. 새 알림 응답은 자동으로 활성화됩니다. 알림 생성을 일시적으로 중단하려면, 알림 응답을 삭제하지 말고 비활성화하면 됩니다.

알림 응답 변경 사항은 즉시 적용되지만, 연결 로그를 SNMP 트랩 또는 시스템 로그 서버로 전송할 때는 예외입니다.

다중 도메인 구축의 경우에는, 알림 응답을 생성하면 해당 응답은 현재 도메인에 속하게 됩니다. 이 알림 응답은 하위 도메인이 사용할 수도 있습니다.

알림 응답 지원 구성

알림 응답 생성이 끝나면 이를 이용해 다음과 같은 외부 알림을 Secure Firewall Management Center에서 전송할 수 있습니다.

알림/이벤트 유형	추가 정보
영향 플래그별 침입 이벤트	영향 플래그 알림 설정, 8 페이지
유형별 검색 이벤트	검색 이벤트 알림 설정, 9 페이지
악성코드 대응 ("네트워크 기반")로 탐지한 악성코드 및 회귀 악성코드 이벤트	악성코드 대응 알림 설정, 9 페이지
상관관계 정책 위반별 상관관계 이벤트	규칙 및 허용 리스트에 응답 추가
로깅 규칙 또는 기본 작업별 연결 이벤트(이메일 알림은 지원되지 않음)	로깅할 수 있는 기타 연결
상태 모듈 및 심각도 수준별 상태 이벤트	상태 모니터 알림 생성

알림 응답 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

SNMP 알림 응답 생성

를 제외하고 디바이스 유형에 대해 SNMPv1, SNMPv2 또는 SNMPv3threat defense를 사용하여 SNMP 알림 응답을 만들 수 있습니다.

참고 SNMP 프로토콜을 위한 SNMP 버전을 선택하는 경우, SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3는 읽기 전용 사용자만 지원한다는 사실을 유념하십시오. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

SNMP로 64비트 값을 모니터링하려는 경우, SNMPv2 또는 SNMPv3을 사용해야 합니다. SNMPv1은 64비트 모니터링을 지원하지 않습니다.

시작하기 전에

- 네트워크 관리 시스템에 Secure Firewall Management Center의 관리 정보 베이스(MIB) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

프로시저

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

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create SNMP Alert(SNMP** 알림 생성**)**을 선택합니다.

단계 **3** SNMP Alert Configuration(SNMP 알림 구성) 필드를 편집합니다.

a) **Name(**이름**)** - SNMP 응답 식별을 위한 이름을 입력합니다.

b) **Trap Server(**트랩 서버**)** - SNMP 트랩 서버의 호스트 이름 또는 IP 주소를 입력합니다.

참고 이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.169.1.456)를 입력한다고 해도 시스템에서 경고하지 않는다는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

c) **Version(**버전**)** - 드롭다운 목록에서 사용하려는 SNMP 버전을 선택합니다. SNMPv3이 기본값입니다.

다음 중에서 선택합니다**.**

- **SNMPv1**or **SNMPv2**: **Community String(**커뮤니티 문자열**)** 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뜁니다.

  참고 SNMP 커뮤니티 문자열 이름에는 특수문자(< > / % # & ? ', 등)를 포함하지 않습니다.

- **SNMP v3**의 경우: **User Name(**사용자 이름**)** 필드에 SNMP 서버로 인증하려는 사용자 이름을 입력하고 다음 단계로 넘어갑니다.

d) **Authentication Protocol(**인증 프로토콜**)** - 드롭다운 목록에서 인증을 암호화하는 데 사용할 프로토콜을 선택합니다.

다음 중에서 선택합니다**.**

- **MD5** — MD5(Message Digest 5) 해시 함수입니다.
- **SHA** — SHA(Secure Hash Algorithm) 해시 함수입니다.

e) **Authentication Password(**인증 비밀번호**)** - 인증을 활성화할 비밀번호를 입력합니다.

f) **Privacy Protocol(**프라이버시 프로토콜**)** —드롭다운 목록에서 개인 비밀번호를 암호화하는 데 사용할 프로토콜을 선택합니다.

다음 중에서 선택합니다**.**

- **DES** - 대칭 비밀 키 블록 알고리즘에서 56비트 키를 사용하는 데이터 암호화 표준(DES)입니다.
- **AES** — 대칭 암호 알고리즘에서 56비트 키를 사용하는 AES(Advanced Encryption Standard)입니다.
- **AES128** — 대칭 암호 알고리즘에서 128비트 키를 사용하는 AES입니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.

g) **Privacy Password(**프라이버시 비밀번호**)** - SNMP 서버에 필요한 프라이버시 비밀번호를 입력합니다. 개인 비밀번호를 지정한 경우 프라이버시가 활성화되며, 인증 비밀번호도 반드시 지정해야 합니다.

h) **Engine ID(**엔진 **ID)** - 짝수를 사용하여 16진법으로 SNMP 엔진을 위한 식별자를 입력합니다.

SNMPv3을 사용할 때, 시스템은 엔진 ID 값을 사용하여 메시지를 암호화합니다. SNMP 서버에서는 메시지를 해독하는 데 이 값이 필요합니다.

Cisco에서는 Secure Firewall Management Center IP 주소의 16진수 버전을 사용할 것을 권장합니다. 예를 들어, Secure Firewall Management Center의 IP 주소가 10.1.1.77이면 0a01014D0을 사용합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

변경 사항은 즉시 적용됩니다. 단,

알림 응답을 사용해 연결 로그를 보내는 경우 해당 알림 응답을 편집한 후 설정 변경 사항을 구축해야 합니다.

시스템 로그 알림 응답 생성

syslog 알림 응답을 설정할 때, syslog 메시지와 연결된 심각도 및 기능을 지정하여 syslog 서버에 의해 제대로 처리되었음을 확인할 수 있습니다. 기능은 메시지를 생성하는 하위 시스템을 나타내며, 심각도는 메시지의 심각도를 정의합니다. 기능 및 심각도는 syslog에 나타나는 실제 메시지에 표시되지 않지만, syslog 메시지를 수신하는 시스템에 메시지 카테고리화 방법을 전달하는 데 사용됩니다.

팁 syslog의 작동 방식 및 구성 방법에 대한 자세한 내용은 시스템에 대한 설명서를 참고하십시오. UNIX 시스템에서는 `syslog` 및 `syslog.conf`의 `man` 페이지에서 개념 정보 및 구성 지침을 제공합니다.

시스템 로그 알림 응답을 생성할 때에는 어떤 유형의 기능이든 선택할 수 있지만, 모든 기능을 지원하는 모든 시스템 로그 서버가 아니라 현재의 시스템 로그 서버를 기반으로 합리적인 하나의 기능을 선택해야 합니다. UNIX syslog 서버의 경우, `syslog.conf` 파일은 어느 기능이 서버의 어느 로그 파일에 저장되는지 나타냅니다.

시작하기 전에

- 이 절차는 다양한 상황의 시스템 로그 메시지를 전송하기 위한 방법으로는 권장하지 않습니다.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.

프로시저

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

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create Syslog Alert(**시스템 로그 알림 생성**)**을 선택합니다.

단계 **3** 알림의 **Name(**이름**)**을 입력합니다.

단계 **4** **Host(**호스트**)** 필드에 시스템 로그 서버의 IP 주소나 호스트 이름을 입력합니다.

참고 이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.168.1.456)를 입력한다고 해도 시스템에서 경고하지 않는다는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

단계 **5** 서버가 시스템 로그 메시지에 사용할 포트를 **Port(**포트**)** 필드에 입력합니다. 기본적으로 이 값은 514로 설정됩니다.

단계 **6** **Facility(**시설**)** 목록에서 시스템 로그 알림 시설, 6 페이지에 설명된 시설을 선택합니다.

단계 **7** **Severity(**심각도**)** 목록에서에 시스템 로그 심각도 레벨, 7 페이지에 설명된 심각도를 선택합니다.

단계 **8** **Tag(**태그**)** 필드에 시스템 로그 메시지와 함께 표시할 태그 이름을 입력합니다.

예를 들어 시스템 로그로 전송된 모든 메시지를 `FromMC` 앞에 오도록 하는 경우, 필드에 `FromMC`를 입력합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

변경 사항은 즉시 적용됩니다. 단,

알림 응답을 사용해 시스템 로그 서버로 연결 로그를 보내는 경우 해당 알림 응답을 편집한 후 설정 변경 사항을 구축해야 합니다.

이 알림 응답을 보안 이벤트를 위해 사용하려는 경우에는, 정책에서 알림 응답을 지정해야 합니다. 보안 이벤트 시스템 로그에 대한 구성 위치의 내용을 참조하십시오.

시스템 로그 알림 시설

다음 표에는 선택 가능한 syslog 기능이 나와 있습니다.

표 *1:* 사용 가능한 ***Syslog*** 기능

기능	설명
ALERT	알림 메시지입니다.
AUDIT	감사 하위 시스템에 의해 생성된 메시지입니다.
AUTH	보안 및 인증과 관련된 메시지입니다.
AUTHPRIV	보안 및 인증과 관련된 제한적 액세스 메시지입니다. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다.
CLOCK	클록 데몬에 의해 생성된 메시지입니다. Windows 운영 체제를 실행하는 syslog 서버는 `CLOCK` 기능을 사용합니다.
CRON	클록 데몬에 의해 생성된 메시지입니다. Linux 운영 체제를 실행하는 syslog 서버는 `CRON` 기능을 사용합니다.
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.

기능	설명
LPR	인쇄 하위 시스템에 의해 생성된 메시지입니다.
MAIL	메일 시스템에 의해 생성된 메시지입니다.
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지입니다.
NTP	NTP 데몬에 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 심각도 레벨

다음 표에는 선택 가능한 표준 syslog 심각도 레벨이 나와 있습니다.

표 *2:* 시스템 로그 심각도 레벨

레벨	설명
ALERT	즉시 해결해야 하는 상태입니다.
CRIT	심각한 상태입니다.
DEBUG	디버깅 정보를 포함하는 메시지입니다.
EMERG	모든 사용자에게 알려진 위험 상태입니다.
ERR	오류 상태입니다.
INFO	정보를 제공하는 메시지입니다.
NOTICE	오류 상태는 아니지만 주의가 필요한 상태입니다.
WARNING	경고 메시지입니다.

이메일 알림 응답 생성

시작하기 전에

- Secure Firewall Management Center이(가) 자체 IP 주소를 역확인할 수 있는지 확인합니다.
- 메일 릴레이 호스트를 메일 릴레이 호스트 및 알림 주소 구성에 설명된 대로 설정합니다.

참고 이메일 알림을 이용해 연결을 기록할 수는 없습니다.

프로시저

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

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create Email Alert(**이메일 알림 생성**)**을 선택합니다.

단계 **3** 알림 응답의 **Name(**이름**)**을 입력합니다.

단계 **4** **To(**수신인**)** 필드에 알림을 전송할 이메일 주소를 쉼표로 구분하여 입력합니다.

단계 **5** **From(**발신인**)** 필드에 알림 전송자로 표시할 이메일 주소를 입력합니다.

단계 **6** **Relay Host(**릴레이 호스트**)** 옆에 나열된 메일 서버가 알림을 전송하는 데 사용하려는 서버인지 확인합니다.

팁 이메일 서버를 변경하려면 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

영향 플래그 알림 설정

특정 영향 플래그의 침입 이벤트가 발생할 때마다 알림을 전송하도록 시스템을 설정할 수 있습니다. 영향 플래그는 침입 데이터, 네트워크 검색 데이터 및 취약성 정보를 상호 연결하여, 침입이 네트워크에 미치는 영향을 평가하는 데 도움이 됩니다.

이러한 알림을 설정하려면 IPS 스마트 라이센스 또는 보호 클래식 라이센스가 있어야 합니다.

프로시저

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

단계 **2** **Impact Flag Alerts(**영향 플래그 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Impact Configuration(**영향 설정**)** 섹션에서 적절한 확인란을 선택하여 각 영향 플래그에 대해 수신할 알림을 지정합니다.

영향 플래그 정의는 침입 이벤트 영향 레벨 섹션을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

검색 이벤트 알림 설정

특정 유형의 검색 이벤트가 발생할 때마다 알리도록 시스템을 설정할 수 있습니다.

시작하기 전에

- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 검색 정책 장에 설명된 대로 알림을 설정할 검색 이벤트 유형을 기록하도록 네트워크 검색 정책을 설정합니다.

프로시저

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

단계 **2** **Discovery Event Alerts(**검색 이벤트 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Events Configuration(**이벤트 설정**)** 섹션에서 각 검색 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

악성코드 대응 알림 설정

악성코드 대응 (네트워크용 AMP)가 회귀 이벤트를 포함한 악성코드 이벤트를 생성할 때마다(즉 "네트워크 기반 악성코드 이벤트"가 생성될 때마다) 알림을 전송하도록 시스템을 설정할 수 있습니다. AMP for Endpoints(엔드포인트용 AMP)("엔드포인트 기반 악성코드 이벤트")가 생성한 악성코드 이벤트에 대한 알림은 만들 수 없습니다.

시작하기 전에

- 악성코드 클라우드 조회를 수행하고 정책을 액세스 컨트롤 규칙과 연결하도록 파일 정책을 설정합니다.자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 액세스 제어 개요를 참조하십시오.
- 이러한 알림을 설정하려면 악성코드 방어 라이선스가 있어야 합니다.

프로시저

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

단계 **2** **Advanced Malware Protections Alerts(**고급 악성코드 보호 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Event Configuration(**이벤트 설정**)** 섹션에서 각 악성코드 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

All network-based malware events(모든 네트워크 기반 악성코드 이벤트**)**에는 **Retrospective Events(**회귀 이벤트**)**가 포함된다는 점에 유의하십시오.

(정의상, 네트워크 기반 악성코드 이벤트는 AMP for Endpoints(엔드포인트용 AMP)가 생성한 이벤트는 포함하지 않습니다.)

단계 **5** **Save(**저장**)**를 클릭합니다.