시스템 구성

다음 항목에서는 Secure Firewall Management Center 및 매니지드 디바이스에 대한 시스템 구성 설정을 구성하는 방법에 대해 설명합니다.

시스템 컨피그레이션 요구 사항 및 전제 조건

모델 지원

Management Center

지원되는 도메인

글로벌

사용자 역할

관리자

시스템 구성 관련 정보

Secure Firewall Management Center에 적용된 시스템 구성 설정입니다.

Secure Firewall Management Center 시스템 구성 탐색

시스템 구성은 management center를 위한 기본적인 설정을 나타냅니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** 탐색 패널을 사용하여 변경할 구성을 선택합니다. 자세한 내용은 표 1: 시스템 구성 설정 , 2 페이지 섹션을 참조하십시오.

시스템 구성 설정

매지니드 디바이스의 경우, 이러한 구성 대부분은 management center에서 적용한 플랫폼 설정 정책으로 처리합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 플랫폼 설정을 참조하십시오.

표 *1:* 시스템 구성 설정

설정	설명
액세스 제어 환경 설정	액세스 제어 정책을 추가하거나 수정할 때 주석을 사용자에게 표시하도록 시스템을 구성합니다. 정책 변경 코멘트, 4 페이지 섹션을 참조하십시오.
검증 번경	지난 24시간 동안 시스템 변경 사항에 대한 상세한 보고서를 보내도록 시스템을 구성합니다. 검증 번경, 2 페이지 섹션을 참조하십시오.
이메일 알림	메일 호스트를 구성하고, 암호화 방법을 선택하고, 이메일 기반 알림 및 보고를 위한 인증 자격 증명을 제공합니다. 이메일 공지, 5 페이지 섹션을 참조하십시오.
침입 정책 환경 설정	사용자가 침입 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성합니다 정책 변경 코멘트, 4 페이지 섹션을 참조하십시오.
네트워크 분석 정책 환경 설정	사용자가 네트워크 분석 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성합니다. 정책 변경 코멘트, 4 페이지 섹션을 참조하십시오.

검증 번경

사용자가 변경하는 내용을 모니터링하고 그러한 변경이 회사의 기본 표준을 따르는지 확인하려면 지난 24시간 동안 변경 사항의 자세한 보고서를 이메일로 전송하도록 시스템을 구성할 수 있습니다. 사용자가 시스템 구성에 변경 사항을 저장할 때마다 변경에 대한 스냅샷이 생성됩니다. 변경 조정 보고서는 이러한 스냅샷의 정보를 결합하여 최신 시스템 변경 사항에 대한 명확한 요약을 제공합니다.

다음 샘플 그림에는 예제 변경 조정 보고서의 User 페이지가 표시되며, 각 구성의 이전 값과 변경 이후의 값이 모두 나열되어 있습니다. 여러 사용자가 동일한 구성을 여러 번 변경하면 보고서에는 최근 것부터 시간순으로 각 변경 사항의 요약이 나열됩니다.

지난 24시간 동안 변경된 내용을 볼 수 있습니다.

검증 변경 구성

시작하기 전에

- 이메일 서버가 24시간 동안 시스템 변경 사항에 대한 이메일 보고서를 수신하도록 구성합니다. 자세한 내용은 메일 릴레이 호스트 및 알림 주소 구성, 5 페이지 섹션을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Configuration**(구성)을(를) 선택합니다.

단계 **2** **Change Reconciliation**(검증 변경)을 클릭합니다.

단계 **3** **Enable**(사용) 확인란을 선택합니다.

단계 **4** 시스템에서 변경 검증 보고서를 전송하도록 할 시간을 **Time to Run**(실행 시간) 드롭다운 목록에서 선택합니다.

단계 **5** **Email to**(수신자) 필드에 이메일 주소를 입력합니다.

팁 이메일 주소를 추가한 후 **Resend Last Report**(마지막 보고서 다시 보내기)를 클릭하여 받는 사람에게 최신 변경 검증 보고서 사본을 전송합니다.

단계 **6** 정책 변경 사항을 포함하려면 **Include Policy Configuration**(정책 구성 포함) 확인란을 선택합니다.

단계 **7** 지난 24시간 동안 모든 변경 사항을 포함하려는 경우 **Show Full Change History**(전체 변경 기록 표시) 확인란을 선택합니다.

단계 **8** **Save**(저장)를 클릭합니다.

관련 항목

감사 로그를 사용하여 변경 검사

검증 변경 옵션

Include Policy Configuration(정책 구성 포함) 옵션은 시스템에 정책 변경 기록이 변경 검증 보고서에 포함되는지 여부를 제어합니다. 여기에는 액세스 제어, 침입, 시스템, 상태 및 네트워크 검색 정책에 대한 변경 사항이 포함됩니다. 이 옵션을 선택하지 않으면 정책에 대한 변경 사항이 보고서에 표시되지 않습니다. 이 옵션은 management center에서만 사용할 수 있습니다.

Show Full Change History(전체 변경 기록 표시) 옵션은 시스템이 변경 검증 보고서에 지난 24시간 동안 발생한 모든 변경 사항의 기록을 포함할지 여부를 제어합니다. 이 옵션을 선택하지 않으면 보고서에는 각 카테고리에 대한 변경 사항의 통합된 보기만 포함됩니다.

참고 변경 조정 보고서에는 threat defense 인터페이스 및 라우팅 설정에 대한 변경 사항이 포함되지 않습니다.

정책 변경 코멘트

사용자가 액세스 제어, 침입 또는 네트워크 분석 정책을 수정할 때 코멘트 기능을 사용하여 여러 정책 관련 변경 사항을 추적하도록 Firepower 시스템을 구성할 수 있습니다.

정책 변경 코멘트를 활성화하면 관리자는 배포의 중요한 정책이 수정된 이유를 신속하게 평가할 수 있습니다. 선택적으로 감사 로그에 작성된 침입 및 네트워크 분석 정책을 변경할 수 있습니다.

정책 변경 추적 코멘트 구성

액세스 제어 정책, 침입 정책 또는 네트워크 분석 정책을 수정할 때 사용자에게 코멘트를 요구하도록 시스템을 구성할 수 있습니다. 코멘트를 사용하여 사용자가 정책을 변경한 이유를 추적할 수 있습니다. 정책 변경에 대한 코멘트를 활성화하는 경우, 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 정책에 대한 새로운 변경 사항이 저장될 때마다 시스템은 사용자에게 코멘트를 입력하라는 메시지를 표시합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

왼쪽된 탐색 패널에서 시스템 구성 옵션이 나타납니다.

단계 **2** 다음 중 하나에 대한 정책 설명 환경설정을 구성합니다.

- 액세스 제어 정책에 대한 설명 환경설정을 보려면 **Access Control Preferences(**액세스 제어 환경설정**)**를 클릭합니다.
- 침입 정책에 대한 설명 환경설정을 보려면 **Intrusion Policy Preferences(**침입 정책 환경설정**)**를 클릭합니다.
- 네트워크 분석 정책에 대한 설명 환경설정을 보려면 **Network Analysis Policy Preferences(**네트워크 분석 정책 환경설정**)**를 클릭합니다.

단계 **3** 각 정책 유형에 대해 다음과 같은 옵션을 선택할 수 있습니다.

- **Disabled(**비활성화**)** - 변경 코멘트를 비활성화합니다.
- **Optional(**선택 사항**)** - 코멘트에서 변경 사항을 설명할 수 있는 옵션을 사용자에게 제공합니다.
- **Required(**필수**)** - 사용자는 저장 전에 코멘트에서 변경 사항을 설명해야 합니다.

단계 **4** 선택적 침입 또는 네트워크 분석 정책 코멘트:

- 모든 침입 정책 변경 사항을 감사 로그에 기록하려면 **Write changes in Intrusion Policy to audit log(**침입 정책의 변경 사항을 감사 로그에 쓰기**)**를 선택합니다.
- 모든 네트워크 분석 정책 변경 사항을 감사 로그에 기록하려면 **Write changes in Network Analysis Policy to audit log(**네트워크 분석 정책의 변경 사항을 감사 로그에 쓰기**)**를 선택합니다.

단계 **5** LSP 업데이트 중에 재정의된 시스템 정의 규칙의 변경 사항에 대한 알림을 받으려면 **Retain user overrides for deleted Snort 3 rules(**삭제된 **Snort 3** 규칙에 대한 사용자 재정의 유지**)** 체크 박스가 선택

되어 있는지 확인합니다. 시스템 기본값으로 이 체크 박스는 선택되어 있습니다. 이 체크 박스를 선택하면 시스템은 LSP 업데이트의 일부로 추가된 새 교체 규칙에서 규칙 재정의를 유지합니다. 알림은 톱니바퀴 (⚙) 옆에 있는 **Tasks(**작업**)** 탭의 알림 아이콘 아래에 표시됩니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이메일 공지

다음을 수행하려는 경우 메일 호스트를 구성합니다.

- 이벤트 기반 보고서 이메일 전송
- 예약 작업에 대한 상태 보고서 이메일 전송
- 변경 검증 보고서 이메일 전송
- 데이터 정리 알림 이메일 전송
- 검색 이벤트, 영향 플래그, 상관 이벤트 알림, 침입 이벤트 알림 및 상태 이벤트 알림에 이메일 사용

이메일 알림을 구성할 때 시스템과 메일 릴레이 호스트 간 통신을 위한 암호화 방법을 선택할 수 있고 필요한 경우 메일 서버의 인증 자격 증명을 제공할 수 있습니다. 구성한 후 연결을 테스트할 수 있습니다.

메일 릴레이 호스트 및 알림 주소 구성

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을 선택합니다.

단계 **2** **Email Notification(**이메일 알림**)**을 클릭합니다.

단계 **3** **Mail Relay Host(**메일 릴레이 호스트**)** 필드에서 사용할 메일 서버의 호스트 이름 또는 IP 주소를 입력합니다. 입력한 메일 호스트는 어플라이언스의 액세스를 허용해야 합니다.

단계 **4** **Port Number(**포트 번호**)** 필드에 이메일 서버에서 사용할 포트 번호를 입력합니다.

일반적인 포트는 다음과 같습니다.

- 25: 암호화를 사용하지 않는 경우
- 465: SSLv3를 사용하는 경우
- 587: TLS를 사용하는 경우

단계 **5** **Encryption(**암호화**)** 방법을 선택합니다.

- **TLS**-전송 계층 보안을 사용하여 통신을 암호화합니다

- **SSLv3**-Secure Socket Layer을 사용 하 여 통신을 암호화 합니다.
- **None (**없음**)**-암호화 되지 않은 통신을 허용 합니다.

참고 어플라이언스와 메일 서버 간의 암호화된 통신에는 인증서 유효성 검사가 필요하지 않습니다.

단계 **6** **From Address(**보낸 사람 주소**)** 필드에 어플라이언스에서 보낸 메시지의 원본 이메일 주소로 사용할 유효한 이메일 주소를 입력합니다.

단계 **7** 선택적으로 메일 서버에 연결할 때 사용자 이름과 비밀번호를 입력하려면 **Use Authentication(**인증 사용**)**을 선택합니다. **Username(**사용자 이름**)** 필드에 사용자 이름을 입력합니다. **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다.

단계 **8** 구성된 메일 서버를 사용하는 테스트 이메일을 전송하려면 **Test Mail Server Settings(**메일 서버 설정 테스트**)**를 클릭합니다.

테스트의 성공 또는 실패를 나타내는 메시지가 버튼 옆에 나타납니다.

단계 **9** **Save(**저장**)**를 클릭합니다.