Firepower Management Center Virtual 초기 관리 및 구성

Firepower Management Center Virtual(FMCv)의 초기 설정 프로세스를 완료하고 성공 여부를 확인한 후, 구축을 쉽게 관리할 수 있게 해주는 다양한 관리 작업을 완료하는 것이 좋습니다. 또한 라이선싱 등 초기 설정 시 건너뛴 작업을 완료해야 합니다. 다음 섹션에서 설명하는 작업에 대한 자세한 내용과 구축 구성을 시작하는 방법에 대한 내용은 사용 중인 버전에 대한 전체 Firepower Management Center 설정 가이드를 참조하십시오.

개인 사용자 계정

초기 설정을 완료하고 나면, 웹 인터페이스 사용자는 시스템에 단 1명만 남게 됩니다. 바로 관리자 역할 및 액세스 권한을 가진 관리자 사용자입니다. 해당 역할의 사용자는 시스템의 모든 메뉴 및 구성에 액세스할 수 있습니다. 보안 및 감사를 위해, 관리자 계정(및 관리자 역할)의 사용은 제한하는 것이 좋습니다. FMC GUI의 **System(**시스템**)** > **Users(**사용자**)** > **User(**사용자**)** 페이지에서 사용자 계정을 관리합니다.

참고 셸을 사용하여 FMC에 액세스하는 관리자 계정은 웹 인터페이스를 사용하여 FMC에 액세스하는 관리자 계정과 다르며, 다른 비밀번호를 사용할 수 있습니다.

시스템을 사용할 각 사용자에 대해 별도의 계정을 만든다면, 조직은 각 사용자의 작업과 각 사용자에 의한 변경 사항을 감사할 수 있을 뿐만 아니라 각 사용자와 관련된 사용자 액세스 역할을 제한할 수 있습니다. 이러한 조치는 대부분의 컨피그레이션 및 분석 작업을 수행하는 FMC에서 특히 중요합니다. 예를 들어, 분석가는 네트워크 보안을 분석하기 위해 이벤트 데이터에 대한 액세스가 필요할 수 있지만 구축 관리 기능에는 액세스가 필요하지 않을 수 있습니다.

시스템에는 웹 인터페이스를 사용하는 다양한 관리자 및 분석가에게 맞게 설계된 10개의 사전 정의된 사용자 역할이 있습니다. 또한 특수 액세스 권한을 가지는 맞춤형 사용자 역할을 생성할 수도 있습니다.

Device Registration

FMC에서는 현재 Firepower System에서 지원하는 모든 디바이스(물리적 또는 가상)를 관리할 수 있습니다.

- Firepower Threat Defense- 통합 차세대 방화벽 및 차세대 IPS 디바이스를 제공합니다.
- Firepower Threat Defense Virtual- 여러 하이퍼바이저 환경에서 작동하도록 설계된 64비트 가상 디바이스는 관리 오버헤드를 줄이고 운영 효율성을 높입니다.
- Cisco ASA with FirePOWER Services(또는 ASA FirePOWER 모듈) - 최우선 시스템 정책을 제공하고 검색 및 액세스 제어를 위해 Firepower System에 트래픽을 전달합니다. 그러나 FMC 웹 인터페이스를 사용하여 ASA FirePOWER 인터페이스를 구성할 수 없습니다. Cisco ASA with FirePOWER Services에는 시스템을 설치하고 기타 플랫폼별 관리 작업을 수행하는 데 사용할 수 있는 ASA 플랫폼에 대해 고유한 CLI 및 소프트웨어가 있습니다.
- 7000 및 8000 Series 어플라이언스 - Firepower System용으로 설계된 물리적 디바이스입니다. 7000 및 8000 Series 디바이스에는 다양한 처리량이 있지만 대부분의 동일한 기능을 공유합니다. 일반적으로 8000 Series 디바이스는 7000 시리즈 디바이스보다 강력하며, 8000 Series fastpath 규칙, 링크 어그리게이션 및 스태킹 등의 추가 기능도 지원합니다. 디바이스를 FMC에 등록하기 전에 반드시 디바이스에 원격 관리를 구성해야 합니다.
- NGIPSv - VMware VSphere 환경에 구축된 64비트 가상 디바이스입니다. NGIPSv 디바이스에서는 이중화 및 리소스 공유, 스위칭, 라우팅과 같은 시스템의 하드웨어 기반 기능을 지원하지 않습니다.

매니지드 디바이스를 FMC에 등록하려면 FMC GUI에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지를 사용해야 합니다. 사용자의 버전에 맞는 Firepower Management Center 구성 가이드에 있는 디바이스 관리 정보를 참조하십시오.

상태 및 시스템 정책

기본적으로, 모든 어플라이언스에는 초기 시스템 정책이 적용되어 있습니다. 시스템 정책은 메일 릴레이 호스트 기본 설정, 시간 동기화 설정 등 구축의 여러 어플라이언스에서 유사할 수 있는 설정을 관리합니다. FMC를 사용하여 FMC 자체와 FMC에서 관리하는 모든 디바이스에 동일한 시스템 정책을 적용하는 것이 좋습니다.

기본적으로, FMC에도 상태 정책이 적용되어 있습니다. 상태 정책은 상태 모니터링 기능에 포함되어 있으며 구축된 어플라이언스의 성능을 지속적으로 모니터링하는 기준을 제공합니다. FMC를 사용하여 여기에서 관리하는 모든 디바이스에 상태 정책을 적용하는 것이 좋습니다.

소프트웨어 및 데이터베이스 업데이트

구축을 시작하기 전에 어플라이언스에서 시스템 소프트웨어를 업데이트해야 합니다. 구축의 모든 어플라이언스에서 최신 버전의 Firepower System을 실행하는 것이 좋습니다. 구축 시 최신 버전을 사용하고 있는 경우 최신 침입 규칙 업데이트, VDB, GeoDB도 설치해야 합니다.

주의 Firepower System의 일부를 업데이트하기 전에 업데이트와 함께 제공되는 릴리스 노트 또는 권고 문구를 읽어야 합니다. 릴리스 정보에는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보가 제공됩니다.

FMC에서 **Firepower** 버전 **6.5** 이상을 실행한다면**,**

구성 중에 FMC에서는 다음 활동을 설정하여 시스템을 최신 상태로 유지하고 데이터를 백업합니다.

- 주간 자동 GeoDB 업데이트
- FMC 및 매니지드 디바이스의 최신 소프트웨어를 다운로드하는 주간 작업

중요 이 작업은 FMC에 대한 소프트웨어 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.

- 로컬에 저장한 구성 전용 FMC 백업을 수행하는 주간 작업

FMC가 **Firepower** 버전 **6.6.** 이상을 사용하고 있을 경우 초기 구성의 일부로서 FMC가 Cisco 지원 사이트에서 최신 취약점 데이터베이스(VDB)를 다운로드하고 설치합니다. 이 작업은 한 번만 수행하면 됩니다.

웹 인터페이스 메시지 센터를 사용하면 이러한 활동의 상태를 확인할 수 있습니다. 시스템이 이러한 활동을 구성하지 못하고 FMC이(가) 인터넷에 액세스할 수 있다면, 사용자의 버전에 맞는 *Firepower Management Center* 구성 가이드의 설명에 따른 활동 구성을 강력하게 권장합니다.

자세한 내용은 자동 초기 구성(버전 6.5 이상) 검토를 참고하십시오.