

FireSIGHT 시스템의 다양한 하드웨어 모델 지원 기능

목차

[소개](#)

[FireSIGHT 시스템의 지원되는 기능](#)

[관련 문서](#)

소개

하드웨어 모델에 따라 FireSIGHT 시스템에서 활성화할 수 있는 기능이 다를 수 있습니다. 이 문서에서는 Cisco FireSIGHT System의 다양한 하드웨어 모델에서 지원되는 기능 및 기능을 간략하게 설명합니다.

참고: 기능을 활성화하려면 FireSIGHT Management Center(Defense Center 또는 DC라고도 함)에 기능 라이선스를 추가한 다음 관리되는 디바이스에 적용해야 합니다. 관리되는 디바이스에 라이선스를 로컬로 설치할 필요가 없습니다.

FireSIGHT 시스템의 지원되는 기능

어플라이언스 모델	FireSIGHT	보호	제어	URL 필터링	악성코드 VPN
관리 어플라이언스	DC750, DC1500, DC3500 (Series 3 Defense Center)	DC750:사용자 2,000명 DC1500:사용자 50,000명 DC3500:사용자 300,000명	이러한 관리 어플라이언스 모델은 모든 관리되는 디바이스 모델(이러한 기능 포함)		
	DC1000, DC3000 (Series 2 Defense Center)	DC1000:사용자 20,000명 DC3000:사용자 100,000명			
	DC500 (Series 2 Defense Center)	DC500:사용자 1,000명 DC500은 FireSIGHT 라이선스가 있는 관리되는 디바이스를 지원하지만 FireSIGHT와 함께 제공되는 지오로케이션 기능은 지원되지 않습니다.			

	습니다.		
가상 방어 센터	Virtual Defense Center 모델은 이러한 기능 중 하나로 모든 관리되는 디바이스 모델을 지원합니다.		
3D7000 시리즈, 3D8000 시리즈 (FirePOWER 디바이스) 3D500, 3D1000, 3D2000 3D2100, 3D2500, 3D3500 3D4500, 3D6500, 3D9900 (Series 2 Device)	FireSIGHT 라이선스는 각 Defense Center 구매에 포함됩니다. 모든 관리 어플라이언스는 관리되는 디바이스 모델을 사용하여 네트워크, 호스트, 애플리케이션 및 사용자 검색을 수행할 수 있습니다.	5.2.x를 실행하는 Series 2 Device에는 보안 인텔리전스 기능을 제외하고 자동 보호 기능이 제공됩니다.	제어 라이선스는 가상 디바이스에서 활성화할 수 있지만 라우팅, 스위칭 또는 NAT와 같은 기본 기능은 사용할 수 없습니다.
관리되는 디바이스		Series 2 Devices는 제어, URL 필터, 악성코드 및 VPN 기능을 지원하지 않습니다.	가상 디바이스는 URL 필터링 및 악성코드 기능을 지원하지 않습니다. VPN은 가상 장치에서 지원되지 않습니다.
가상 디바이스	가상 디바이스 내용은 DC(위)의 FireSIGHT 섹션을 참조하십시오.	가상 디바이스 모델은 보호 기능을 지원합니다.	

참고: 레거시 RNA 및 RUA 기능 라이선스는 DC500, DC1000 및 DC3000 모델에서 지원할 수 있습니다. 그러나 FireSIGHT Management Center의 하드웨어 기능과 일치하는 사용자 제한을 초과하지 않는 것은 권장하지 않습니다.

관련 문서