Funciones y capacidades admitidas de varios modelos de hardware del sistema FireSIGHT

Contenido

[Introducción](#)
[Funciones y capacidades admitidas de los sistemas FireSIGHT](#)
[Artículos relacionados](#)

Introducción

Según el modelo de hardware, las funciones que puede activar en un sistema FireSIGHT pueden ser diferentes. Este documento proporciona una descripción general de las funciones y capacidades soportadas de varios modelos de hardware de Cisco FireSIGHT System.

> **Nota:** Para habilitar una función, debe agregar una *licencia de función* en un FireSIGHT Management Center (también conocido como Defense Center o DC) y aplicarla en un dispositivo administrado. No es necesario instalar ninguna licencia localmente en un dispositivo administrado.

Funciones y capacidades admitidas de los sistemas FireSIGHT

Dispositivo	Modelo	FireSIGHT	Protección	Control	Filtrado de URL	Malware VP
Dispositivo de administración	DC750, DC1500, DC3500 (Centro de defensa serie 3) DC1000, DC3000 (Centro de defensa serie 2)	DC750: 2000 usuarios DC1500: 50 000 usuarios DC3500: 300 000 usuarios DC1000: 20 000 usuarios DC3000: 100 000 usuarios	Estos modelos de dispositivo de administración son compati todos los modelos de dispositivos administrados con cualqu estas funciones.			
	DC500 (Centro de defensa serie 2)	DC500: 1000 usuarios DC500 admite dispositivos administrados con licencia FireSIGHT, pero no se admite la funcionalidad	DC500 admite dispositivos administrados con licencia de protección, pero la función de inteligencia de seguridad no es compatible.	DC500 admite dispositivos administrados con licencia de control, pero la función Control de usuario no es	Not Supported	El r DC adr fun VP

		de geolocalización que incluye FireSIGHT.		compatible.	
	Centro de defensa virtual	El modelo de Virtual Defense Center es compatible con todos los modelos d dispositivos administrados con cualquiera de estas funciones.			
	Serie 3D7000 , Serie 3D8000 (Dispositivo FirePOWER)	Cada compra de Defense Center incluye una licencia de FireSIGHT.	Los dispositivos FirePOWER admiten todas estas funciones		
Dispositivo administrado	3D500, 3D1000, 3D2000 3D2100, 3D2500, 3D3500 3D4500, 3D6500, 3D9900 (Dispositivo de la serie 2)	Todos los dispositivos de gestión tienen la capacidad de realizar la detección de redes, hosts, aplicaciones y usuarios mediante cualquier modelo de dispositivo administrado.	Un dispositivo de la serie 2 que ejecuta 5.2.x tiene la función de protección automáticamente, a excepción de la función de inteligencia de seguridad.	Los dispositivos de la serie 2 no admiten funciones de control, filtrado de URL, mal VPN.	
	Dispositivo virtual	La limitación de una licencia de FireSIGHT depende de los modelos de CC. Consulte la sección FireSIGHT del DC (anterior) para obtener más información.	El modelo de dispositivo virtual admite la función de protección.	La licencia de control se puede habilitar en un dispositivo virtual, pero ninguna función de base de hardware, como Routing, Switching o NAT, está disponible.	Los dispositivos virtuales admiten funciones de filtrado de URL y malware.

Nota: Los modelos DC500, DC1000 y DC3000 admiten licencias de funciones de RNA y RUA antiguas. Sin embargo, Cisco no recomienda superar los límites de usuario que coinciden con las capacidades de hardware de los FireSIGHT Management Centers.

Artículos relacionados