Guía breve para el usuario de Cisco Secure Firewall 200 Series

Última modificación: 2026-03-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CISCO SYSTEMS DE MEXICO S.DE R.L. DE C.V.

Avenida (AV) Paseo de Tamarindos 400A, piso 14

Col. Bosques de las Lomas, Cuajimalpa de Morelos

Mexico, Ciudad De Mexico 05120

Tel: +52 55 5267 1000

LAS ESPECIFICACIONES E INFORMACIÓN RELATIVAS A LOS PRODUCTOS DE ESTE MANUAL ESTÁN SUJETAS A CAMBIOS SIN PREVIO AVISO. TODAS LAS DECLARACIONES, INFORMACIONES Y RECOMENDACIONES INCLUIDAS EN ESTE MANUAL SE CONSIDERAN PRECISAS; SIN EMBARGO, NO SE PRESENTAN GARANTÍAS DE NINGÚN TIPO, NI EXPRESAS NI IMPLÍCITAS. LOS USUARIOS DEBEN ASUMIR LA PLENA RESPONSABILIDAD DE SU APLICACIÓN EN TODOS LOS PRODUCTOS.

LA LICENCIA DE SOFTWARE Y LA GARANTÍA LIMITADA DEL PRODUCTO AL QUE ACOMPAÑAN SE EXPONEN EN EL PAQUETE DE INFORMACIÓN QUE SE ENVÍA CON EL PRODUCTO Y SE INCLUYEN EN EL PRESENTE DOCUMENTO A TRAVÉS DE ESTA REFERENCIA. SI NO ENCUENTRA LA LICENCIA DEL SOFTWARE O LA GARANTÍA LIMITADA, PÓNGASE EN CONTACTO CON SU REPRESENTANTE DE CISCO PARA OBTENER UNA COPIA.

La siguiente información concierne al cumplimiento de los requisitos de la FCC para los dispositivos de Clase A: este equipo ha sido probado y cumple con los límites establecidos para un dispositivo digital de Clase A, de conformidad con el apartado 15 del reglamento de la FCC. Estos límites están diseñados para proporcionar una protección razonable frente a cualquier interferencia perjudicial al utilizar el equipo en un entorno comercial. Este equipo genera, usa y puede emitir energía de radiofrecuencia y, en caso de no instalarse ni usarse de conformidad con el manual de instrucciones, podría causar interferencias perjudiciales que dificultarían las comunicaciones por radio. La conexión de este equipo en una zona residencial puede provocar interferencias perjudiciales; en tal caso, se exigirá a los usuarios que corran con los gastos de la reparación de dichos daños.

La siguiente información concierne al cumplimiento de los requisitos de la FCC para los dispositivos de Clase B: este equipo ha sido probado y cumple con los límites establecidos para un dispositivo digital de Clase B, de conformidad con el apartado 15 del reglamento de la FCC. Estos límites han sido diseñados con el objetivo de proporcionar una protección razonable frente a interferencias perjudiciales en instalaciones residenciales. Este equipo genera, usa y puede emitir energía de radiofrecuencia y, en caso de no instalarse ni usarse de conformidad con las instrucciones, podría causar interferencias perjudiciales que dificultarían las comunicaciones por radio. Sin embargo, no es posible garantizar que no vayan a producirse interferencias en una instalación determinada. Si el equipo causa interferencias en la recepción de señales de radio o televisión (lo que se puede determinar apagando y encendiendo el equipo), se recomienda a los usuarios que intenten corregir las interferencias mediante uno o varios de los métodos que se indican a continuación:

- Reoriente o reubique la antena receptora.
- Aumente la distancia entre los equipos y el receptor.
- Conecte el equipo a una toma en un circuito diferente al que se encuentra conectado el receptor.
- Solicite ayuda al distribuidor o a un técnico experto en radio y televisión.

Las modificaciones realizadas en el producto que no estén autorizadas por Cisco podrían anular la aprobación de la FCC y negarle el permiso para utilizar el producto.

La implementación por parte de Cisco de la compresión del encabezado de TCP es una adaptación de un programa desarrollado por la Universidad de California, Berkeley (UCB) como parte de la versión de dominio público del sistema operativo UNIX de la UCB. Todos los derechos reservados. Copyright © 1981, Regentes de la Universidad de California.

NO OBSTANTE CUALQUIER OTRA GARANTÍA QUE AQUÍ SE DESCRIBA, TODOS LOS ARCHIVOS DE DOCUMENTO Y SOFTWARE DE ESTOS PROVEEDORES SE PROPORCIONAN "TAL CUAL" CON TODOS LOS ERRORES QUE PUDIERAN INCLUIR. CISCO Y LOS PROVEEDORES ANTERIORMENTE MENCIONADOS NIEGAN CUALQUIER GARANTÍA, EXPRESA O IMPLÍCITA, INCLUIDAS, SIN LIMITACIÓN, AQUELLAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN DETERMINADO E INCUMPLIMIENTO O QUE PUEDAN SURGIR DE UN PROCESO DE NEGOCIACIÓN, USO O PRÁCTICA COMERCIAL.

BAJO NINGUNA CIRCUNSTANCIA CISCO O SUS PROVEEDORES SERÁN RESPONSABLES DE NINGÚN DAÑO INDIRECTO, ESPECIAL, SECUNDARIO O FORTUITO, INCLUIDOS ENTRE OTROS, LA PÉRDIDA DE GANANCIAS, O LA PÉRDIDA O EL DAÑO DE DATOS COMO CONSECUENCIA DEL USO O INCAPACIDAD DE USO DE ESTE MANUAL, INCLUSO EN EL CASO DE QUE CISCO O SUS PROVEEDORES HAYAN SIDO NOTIFICADOS SOBRE LA POSIBILIDAD DE QUE SE PRODUZCAN TALES DAÑOS.

Cualquier dirección de protocolo de Internet (IP) o número de teléfono utilizado en este documento no pretende ser una dirección o un número de teléfono real. Cualquier ejemplo, salida de visualización de comandos, diagrama de topología de red y figura incluida en el documento se muestra solo con fines ilustrativos. El uso de direcciones IP o números de teléfono reales en el material ilustrativo no es intencionado, sino mera coincidencia.

Se carece de control sobre todas las copias impresas y duplicados en formato electrónico de este documento. Consulte la versión en línea actual para obtener la versión más reciente.

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

CAPÍTULO 1

Guía breve para el usuario de Cisco Secure Firewall 200 Series

- Características, en la página 1
- Ubicaciones del bloqueo Kensington, de la etiqueta de cumplimiento, de la etiqueta “No apilar”, de la etiqueta de advertencia de sistema caliente y del código QR del portal de documentación digital, en la página 1
- Panel frontal, en la página 3
- Panel posterior, en la página 3
- LED del panel posterior, en la página 3
- Puerto de administración, puertos de consola y puerto USB, en la página 3
- Botón de encendido y botón de reinicio, en la página 4
- Especificaciones de hardware, en la página 5
- Transceptores compatibles, en la página 5
- Colocación, en la página 7
- Producto de clase A, en la página 7
- Almacenamiento, transporte, venta y eliminación , en la página 7
- Qué hacer si el equipo funciona mal, en la página 7
- Información adicional, en la página 8

Características

El Cisco Secure Firewall 200 Series es una adición rentable y altamente eficaz a nuestra familia de firewalls de gama baja. Está diseñado para sucursales empresariales, negocios del sector minorista y ubicaciones pequeñas, y ofrece seguridad resistente y asequible con inteligencia de amenazas avanzada, características de seguridad en la nube y rendimiento optimizado para una protección integral de nivel empresarial.

Consulte la Guía de compatibilidad de Cisco Secure Firewall Threat Defense y Compatibilidad de Cisco Secure Firewall ASA, que brindan la compatibilidad de software y hardware de Cisco Firewall, incluidos los requisitos del entorno de alojamiento y sistema operativo, para cada versión admitida de Firewall.

Ubicaciones del bloqueo Kensington, de la etiqueta de cumplimiento, de la etiqueta “No apilar”, de la etiqueta de

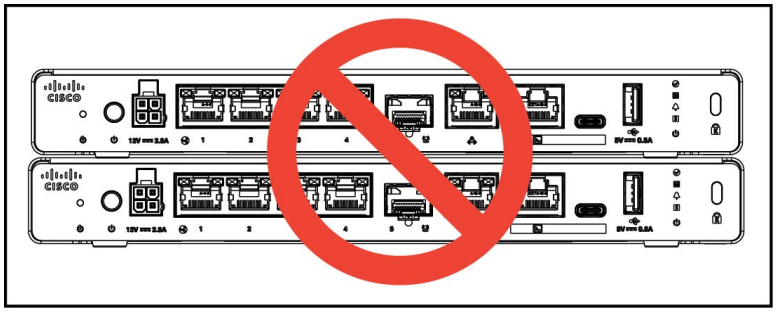
advertencia de sistema caliente y del código QR del portal de documentación digital

El chasis tiene un bloqueo Kensington que acepta un mecanismo de bloqueo de barra en T estándar de Kensington para asegurar el chasis.

La etiqueta de cumplimiento en la parte inferior del chasis contiene el número de serie del chasis, las marcas de cumplimiento normativo y el código QR del portal de documentación digital que remite a la guía de introducción, la guía reglamentaria y de cumplimiento, la guía de aprovisionamiento automatizado y la guía de instalación del hardware.

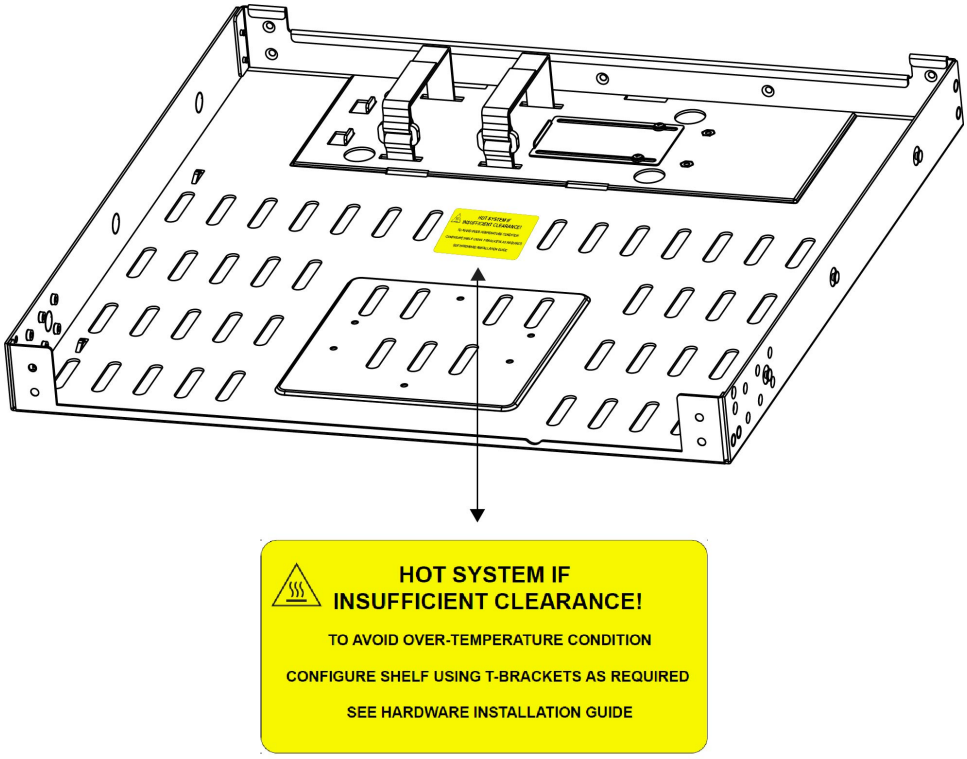
La etiqueta "No apilar" se encuentra en la parte superior de la cubierta del chasis. En la siguiente figura se muestra la etiqueta "No apilar".

Figura 1: Etiqueta "No apilar" en el chasis



La etiqueta de advertencia de sistema caliente se encuentra en la bandeja de montaje en rack, como se muestra en la figura siguiente.

Figura 2: Etiqueta de advertencia de sistema caliente en la bandeja de montaje en rack



Panel frontal

Panel posterior

LED del panel posterior

Puerto de administración, puertos de consola y puerto USB

Puerto de administración

El chasis de la serie tiene un puerto de administración Cisco RJ-45 de 1 Gbps. Este puerto está restringido al acceso de administración de redes y se conecta con un cable RJ-45.

Puertos de consola RJ-45

tiene dos puertos de consola externos, un puerto serial Cisco RJ-45 y un puerto serial USB tipo C. Solo puede estar activo un puerto de consola a la vez. Cuando se conecta un cable al puerto de consola USB, el puerto RJ-45 queda inactivo. En cambio, cuando se quita el cable USB del puerto USB, el puerto RJ-45 se activa. Los puertos de consola no tienen ningún control de flujo de hardware. Puede utilizar la

CLI para configurar el chasis a través del puerto de consola serial mediante un servidor de terminal o un programa de emulación de terminales en una computadora.

- Puerto RJ-45 (8P8C): admite la señalización RS-232 a un controlador UART interno. El puerto de consola RJ-45 no admite un módem de marcación remota. Puede utilizar adaptador para convertir la conexión de RJ45 en DB9 si es necesario.
- Puerto USB tipo C: permite la conexión a un puerto USB de una computadora externa. Puede enchufar y desenchufar el cable USB del puerto de consola sin afectar las operaciones de Windows HyperTerminal. Recomendamos cables USB blindados con blindajes debidamente terminados. La configuración predeterminada es 9600 baudios. Utilícelo para la conexión inicial. Las velocidades en baudios para el puerto de consola USB son 1200, 2400, 4800, 9600, 19 200, 38 400, 57 600 y 115 200 bps.

Puerto USB 3.0 tipo A

proporciona un puerto USB 3.0 tipo A que se puede usar para conectar un dispositivo externo. El puerto USB puede brindar una potencia de salida de 5 V y hasta un máximo de 0,5 A, y 2,5 W de potencia.

- Unidad USB externa (opcional): puede utilizar el puerto USB tipo A externo para conectar un dispositivo de almacenamiento de datos. El identificador de la unidad USB externa es *disk1*. Cuando se enciende el chasis, se monta una unidad USB conectada como disk1 y está disponible para su uso. Además, los comandos del sistema de archivos que están disponibles para disk0 también están disponibles para disk1, incluidos **copy**, **format**, **delete**, **mkdir**, **pwd**, **cd**, etc.
- Sistema de archivos FAT-32: solo admiten sistemas de archivos con formato FAT-32 para la unidad USB externa. Si inserta una unidad USB externa que no está en formato FAT-32, el proceso de montaje del sistema falla y usted recibe un mensaje de error. Puede ingresar el comando **format disk1:** para formatear la partición en FAT-32 y montar la partición en disk1 nuevamente. Sin embargo, es posible que se pierdan datos.

Botón de encendido y botón de reinicio

Botón de encendido

El botón pulsador de encendido está ubicado en el lado izquierdo del panel posterior. Controla la alimentación del sistema. Cuando se enciende la alimentación de CA por primera vez, no es necesario presionar el botón de encendido porque el sistema se activa de manera predeterminada. El sistema está APAGADO cuando el botón sobresale y ENCENDIDO cuando el botón se presiona. Durante el proceso de apagado, el LED de alimentación parpadea en verde para indicar que el proceso ha comenzado. Una vez que se completa el apagado, el sistema se desconecta. Espere que los LED de alimentación del sistema se apaguen antes de desconectar los cables de alimentación de CA. Consulte LED del panel posterior, en la página 3 para obtener una descripción detallada del LED de estado de alimentación.

En el indicador de ROMMON o FX-OS:

- Presione el botón de encendido durante 5 segundos y suéltelo para iniciar un ciclo de encendido. El LED de alimentación parpadea en verde a una frecuencia de 2 Hz.
- Presione el botón de encendido durante 15 segundos y suéltelo para iniciar un apagado correcto. El LED de alimentación parpadea en verde a una frecuencia de 10 Hz.

Nota Threat Defense requiere un apagado correcto. Consulte la Guía de introducción para conocer el procedimiento.

Precaución Si desconecta los cables de alimentación del sistema antes de que se complete el apagado correcto, el disco puede dañarse. Puede mover el switch de alimentación a la posición APAGADO antes de apagar el sistema. El sistema lo ignora.

Nota Después de desconectar la alimentación del chasis desenchufando el cable de alimentación, espere al menos 10 segundos antes de volver a conectar la alimentación. Es necesario mantener apagado el sistema, incluida la alimentación en espera, durante 10 segundos.

Botón de restablecimiento de fábrica

El chasis tiene un botón de restablecimiento empotrado que restablece el sistema a los valores predeterminados de fábrica. Presione y mantenga presionado el botón con un alfiler durante cinco segundos para restablecer el chasis a su estado predeterminado después del siguiente reinicio.

Nota Utilice el botón de restablecimiento si se pierden las credenciales actuales y desea inicializar la casilla sin tener acceso a la consola.

Nota Las variables de configuración se restablecen a los valores predeterminados de fábrica, pero la memoria flash no se borra ni se elimina ningún archivo.

Nota Si se pierde la alimentación entre el momento en que presionó el botón de restablecimiento y el momento en que se completa el proceso de restablecimiento, el proceso se detiene y debe presionar el botón nuevamente después de que el sistema se vuelve a encender.

Especificaciones de hardware

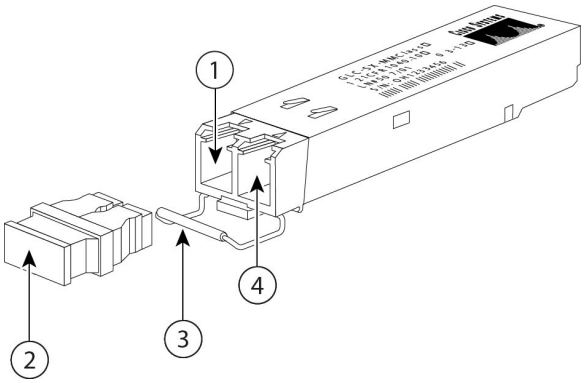
Transceptores compatibles

El transceptor SFP es un dispositivo bidireccional que tiene un transmisor y un receptor en el mismo paquete físico. Es una interfaz óptica o eléctrica (de cobre) intercambiable en caliente que se conecta a los puertos SFP en los puertos fijos y proporciona conectividad Ethernet.

Consulte la Ficha técnica de los módulos SFP de Cisco para aplicaciones Gigabit Ethernet para obtener más información.

En la siguiente figura, se muestran los componentes de un transceptor.

Figura 3: Transceptor SFP



1	Orificio óptico de recepción	**2**	Funda
3	Cierre de fianza	**4**	Orificio óptico de transmisión

Advertencias de seguridad

Tenga en cuenta las siguientes advertencias:

Advertencia La radiación por láser invisible está presente. No exponga a los usuarios de telescopios ópticos. Esto se aplica a los productos láser de clase 1 y 1M.

Advertencia Puede que se emita radiación láser invisible desde el final del cable de fibra o conector sin terminal. No lo mire directamente con instrumentos ópticos. Mirar la salida láser con determinados instrumentos ópticos (por ejemplo, lupas binoculares o de aumento y microscopios) a una distancia de 100 mm puede ser peligroso para los ojos.

Advertencia El uso de controles, ajustes o bien la realización de procedimientos distintos a los especificados, pueden provocar la exposición a radiación peligrosa.

Advertencia Utilice los procedimientos ESD adecuados al insertar el transceptor. Evite tocar los contactos en la parte posterior y mantenga los contactos y los puertos libres de polvo y suciedad. Mantenga los transceptores no utilizados en el paquete de ESD en el que se enviaron.

Precaución Aunque se permiten los SFP que no son de Cisco, no recomendamos su uso porque no han sido probados ni validados por Cisco. El Centro de Asistencia Técnica (TAC) de Cisco puede negar el soporte ante cualquier problema de interoperabilidad que resulte del uso de un transceptor SFP de terceros no probado.

Colocación

Este equipo está diseñado para uso industrial y comercial en entornos libres de riesgos para la salud y la seguridad. Se permite el funcionamiento sin supervisión continua. La instalación y el mantenimiento del equipo deben estar a cargo de personal debidamente calificado con los conocimientos y las habilidades suficientes.

Producto de clase A

Este producto puede causar interferencias de radio en un entorno doméstico, en cuyo caso puede ser necesario que el usuario tome las medidas adecuadas.

Almacenamiento, transporte, venta y eliminación

Almacene el equipo en el interior en su embalaje original.

- Rango de temperatura de almacenamiento (cuando está apagado): -25 °C a 70 °C
- Rango de humedad relativa (cuando está apagado): 5 % a 95 % sin condensación

Transporte el equipo en su embalaje original dentro de vehículos cerrados en cualquier medio de transporte.

- Rango de temperatura de transporte: -25 °C a 70 °C
- Rango de humedad relativa: 5 % a 85 % sin condensación

Los términos y condiciones en los que se vende el equipo se rigen por los contratos entre Cisco o los partners autorizados de Cisco y los compradores de los equipos.

La eliminación del equipo en el fin de la vida útil debe realizarse en cumplimiento de todas las leyes y normativas nacionales aplicables.

Qué hacer si el equipo funciona mal

Si experimenta problemas de funcionamiento del equipo o desea presentar un reclamo sobre la calidad, comuníquese con su proveedor de equipos.

También puede encontrar información sobre el soporte técnico de Cisco en su sitio web oficial:

https://www.cisco.com/c/es_mx/index.html

La garantía del fabricante establece que el equipo cumple con las especificaciones de la etiqueta siempre que se haya almacenado, transportado, instalado y operado según la documentación técnica asociada.

La garantía y el soporte de servicio no se aplican al equipo en los siguientes casos:

- Si ha sufrido cambios, modificaciones, manejo incorrecto, destrucción o daños debido a cualquiera de las siguientes condiciones:
  - Causas naturales
  - Exposición ambiental
  - No tomar las medidas requeridas
  - Negligencia, actos intencionales o uso indebido
  - Uso para fines distintos a los especificados en la documentación correspondiente
  - Acto u omisión de un tercero
  - Signos de haber sido sometido a fuego, agua, sustancias químicas, incluida pero no limitada a la aplicación de pintura y otros tipos de revestimientos
  - Reparación o modificaciones internas no autorizadas
  - Daño mecánico
  - Signos de entrada de objetos extraños, líquidos o insectos
  - Daños causados por el incumplimiento de las regulaciones técnicas existentes, las normas estatales, las regulaciones relacionadas con el funcionamiento del hardware en una red de comunicaciones pública y otros requisitos oficiales aplicables para los parámetros de redes de alimentación, telecomunicaciones y cable, así como otros factores externos similares

Información adicional

Para obtener instrucciones de instalación más detalladas, consulte las guías de instalación en el sitio web oficial de Cisco:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/200/hw-install-200.html

https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/secure-firewall-aag.html

https://www.cisco.com/c/en/us/support/security/secure-firewall-200-series/products-installation-guides-list.html

Acerca de la traducción

Es posible que Cisco proporcione traducciones de este contenido al idioma local en algunas ubicaciones. Tenga en cuenta que las traducciones se ofrecen únicamente con fines informativos y, si hubiera alguna discrepancia, prevalecerá la versión en inglés del contenido.