Cisco Stealthwatch

Guía de instalación de hardware de la serie x210

Table of Contents

Introducción

Descripción general

En esta guía, se explica cómo instalar appliances de hardware de la serie x210 de Stealthwatch. Se describen los componentes de Stealthwatch y cómo se sitúan en el sistema, incluida la integración de sensores de flujo. En esta guía, también se describe el montaje y la instalación del hardware de Stealthwatch. El hardware de la serie x210 incluye:

Appliance	Número de pieza
Recopilador de flujo 4210 de Stealthwatch	ST-FC4210-K9
Motor del recopilador de flujo 5210 de Stealthwatch	ST-FC5210-E
Base de datos del recopilador de flujo 5210 de Stealthwatch	ST-FC5210-D
Sensor de flujo 1210 de Stealthwatch	ST-FS1210-K9
Sensor de flujo 3210 de Stealthwatch	ST-FS3210-K9
Sensor de flujo 4210 de Stealthwatch	ST-FS4210-K9
Consola de gestión 2210 de Stealthwatch	ST-SMC2210-K9
UDP Director 2210 de Stealthwatch	ST-UDP2210-K9

Público

Esta guía está diseñada para la persona responsable de la instalación del hardware de Stealthwatch. Damos por sentado que ya dispone de ciertos conocimientos generales sobre la instalación de equipos de red (sensor de flujo, recopilador de flujo, UDP Director y consola de gestión de Stealthwatch).

> Para obtener información sobre la configuración de appliances de Stealthwatch, consulte la **Guía de instalación y configuración de Stealthwatch** correspondiente a su versión de software. La serie x210 es compatible con las versiones de software 7.x de Stealthwatch.

Utilización de esta guía

Además de esta introducción, hemos dividido esta guía en los siguientes capítulos:

Capítulo	Descripción
2 - **Consideraciones previas a la configuración**	Componentes de Stealthwatch, su ubicación y configuración del firewall para las comunicaciones
3 - **Preparación de la instalación**	Pautas, advertencias y recomendaciones de seguridad
4 - **Instalación**	Montaje e instalación del hardware de Stealthwatch

Abreviaturas frecuentes

En esta guía, se incluyen las siguientes abreviaturas:

Abreviatura	Descripción
DMZ.	Zona desmilitarizada (una red perimetral)
HTTPS	Protocolo (seguro) de transferencia de hipertexto
ISE	Identity Services Engine (ISE)
NIC	Tarjeta de interfaz de red
NTP	Protocolo de tiempo de red
PCIe	Interconexión rápida de componentes periféricos
SNMP	Protocolo simple de administración de red
SPAN	Analizador de puerto de switch
TAP	Puerto de acceso de prueba
UPS	Fuente de alimentación ininterrumpida
VLAN	Red de área local virtual

Preparación de instalación

Advertencias de instalación

Lea el documento Información de seguridad normativa y de cumplimiento antes de instalar los appliances de la serie Stealthwatch x210.

Tome nota de las siguientes advertencias:

Advertencia 1071: definición de advertencia

INSTRUCCIONES DE SEGURIDAD IMPORTANTES

Este símbolo de advertencia indica peligro. Puede sufrir lesiones físicas. Antes de manipular cualquier equipo, debe ser consciente de los peligros que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Utilice el número de advertencia que aparece al final de cada una para localizar su traducción en las advertencias de seguridad que acompañan a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Advertencia 1005: disyuntor del circuito

Este producto utiliza el sistema de protección contra cortocircuitos (sobretensión) instalado en el edificio. Asegúrese de que el dispositivo de protección no sea superior a: EU: 250 V, 16 A (EE. UU.: 120, 15 A)

Advertencia 1004: instrucciones de instalación

Lea las instrucciones de instalación antes de usar, instalar o conectar el sistema a la fuente de alimentación.

Advertencia 12: advertencia de desconexión de la fuente de alimentación

Antes de trabajar en un chasis o cerca de fuentes de alimentación, desconecte el cable de alimentación de las unidades de CA; desconecte la alimentación del las unidades de CC en el disyuntor de circuitos.

Advertencia 43: advertencia de retirada de joyas

Antes de comenzar a trabajar con el equipo conectado a las líneas de alimentación, quítese las joyas (incluidos anillos, collares y relojes). Los objetos metálicos se calientan cuando están conectados a una fuente de alimentación y a tierra, y pueden provocar quemaduras graves o que el objeto metálico se suelde a los terminales.

Advertencia 94: advertencia de la correa de muñeca

Durante este procedimiento, utilice correas de muñecas para evitar daños por descarga electrostática en la tarjeta. No toque directamente la placa base con la mano o cualquier herramienta metálica o podría electrocutarse.

Advertencia 1045: protección contra cortocircuitos

Este producto requiere protección contra cortocircuitos (sobretensión), que se suministra como parte de la instalación del edificio. Instale solo conforme a las normativas de cableado locales y nacionales.

Advertencia 1021: circuito SELV

Con el fin de evitar descargas eléctricas, no conecte circuitos de voltaje extrabajo de seguridad (SELV) a los circuitos de voltaje de la red telefónica (TNV). Los puertos LAN contienen circuitos SELV, mientras que los puertos WAN tienen circuitos TNV. Algunos puertos, tanto LAN como WAN, utilizan conectores RJ-45. Tenga cuidado al conectar los cables.

Advertencia 1024: conductor de puesta a tierra

Este equipo debe conectarse a tierra. No desactive nunca el conductor de puesta a tierra ni utilice el equipo sin un conductor de puesta a tierra correctamente instalado. Póngase en contacto con la autoridad de inspección eléctrica pertinente o con un electricista si no está seguro de contar con una conexión a tierra apropiada.

Advertencia 1040: eliminación del producto

Al desechar este producto deben tenerse en cuenta todas las leyes y normativas nacionales.

Advertencia 1074: cumplimiento de los códigos eléctricos locales y nacionales

La instalación del equipo debe cumplir con los códigos eléctricos locales y nacionales.

Advertencia 19: advertencia sobre alimentación de TN

El dispositivo ha sido diseñado para trabajar con sistemas de alimentación TN.

Instrucciones de instalación

Tome nota de las siguientes advertencias:

Declaración 1047: prevención contra sobrecalentamiento

Para evitar que el sistema se sobrecaliente, no lo utilice en una zona que supere la temperatura ambiente máxima recomendada de: 5 a 35 °C (41 a 95 °F)

Advertencia 1019: dispositivo de desconexión principal

La combinación de la caja de enchufe debe estar siempre accesible porque sirve como dispositivo principal de desconexión.

Advertencia 1005: disyuntor del circuito

Este producto utiliza el sistema de protección contra cortocircuitos (sobretensión) instalado en el edificio. Asegúrese de que el dispositivo de protección no sea superior a: EU: 250 V, 16 A (EE.UU.: 120, 15 A)

Advertencia 1074: cumplimiento de los códigos eléctricos locales y nacionales

La instalación del equipo debe cumplir con los códigos eléctricos locales y nacionales.

Advertencia 371—Cable de alimentación y adaptador de CA

Utilice los cables de conexión/cables de alimentación/adaptadores de corriente alterna/baterías proporcionados o designados cuando instale el producto. Usar cualquier otro cable o adaptador podría provocar un error o un incendio. La ley de seguridad de aparatos y materiales eléctricos prohíbe el uso de cables con la certificación UL (aquellos que lleven las marcas “UL” o “CSA” en el cable), que no estén sujetos a dicha ley y por la cual debe figurar “PSE” en el cable, en ningún dispositivo eléctrico que no sean los productos designados por CISCO.

Advertencia 1073: ninguna pieza que el usuario pueda reparar

Ninguna pieza interior del dispositivo puede ser reparada por el usuario. No abrir.

Cuando instale un chasis, utilice las siguientes directrices:

- Asegúrese de que hay un espacio adecuado alrededor del chasis para permitir el mantenimiento y un flujo de aire adecuado. El flujo de aire en el chasis va desde la parte frontal a la trasera.

  Para asegurar el flujo de aire adecuado es necesario asegurar su chasis con un kit de raíles. La colocación física de las unidades una encima de otra o el apilamiento sin el uso de los kit de raíles bloquea las ranuras de ventilación encima del chasis, lo que podría dar como resultado sobre-calentamiento, velocidades del ventilador más altas y un mayor consumo energético Le recomendamos que monte su chasis en los kit de raíles cuando los instale en el rack, ya que estos raíles ofrecen el espaciado mín-imo necesario entre los chasis. No se necesita un espaciado adicional entre el chasis cuando los monte utilizando kit de raíles.

- Asegúrese de que el aire acondicionado puede mantener el chasis a una tem-peratura de 5 a 35 °C (41 a 95 °F).
- Asegúrese de que el armario o rack cumple con los requisitos del rack.
- Asegúrese de que la alimentación del sitio cumple con los requisitos de ali-mentación que aparecen en la hoja de especificaciones para su appliance. Si está disponible, puede utilizar un UPS para protegerse frente a fallos de alimentación.

  Evite las UPS que utilizan la tecnología ferrorresonante. Este tipo de UPS pueden volverse inestables con estos sistemas, que pueden tener

importantes fluctuaciones de toma de corriente de patrones de trafico de datos fluctuantes.

Recomendaciones de seguridad

La siguiente información le ayuda a garantizar su seguridad y a proteger el chasis. Puede que esta información no sea aplicable a todas las situaciones potencialmente peligrosas de su entorno de trabajo, así que esté atento y siga siempre un buen criterio.

Tenga en cuenta estas directrices de seguridad:

- Mantenga el área limpia y sin polvo antes, durante y después de la instalación.
- Mantenga las herramientas fuera de las zonas de paso donde usted u otras personas podrían tropezarse.
- No lleve ropa holgada ni joyas como pendientes, pulseras o cadenas que puedan engancharse en el chasis.
- Utilice gafas de seguridad si trabaja en cualquier condición que pueda ser peligrosa para sus ojos.
- No realice ninguna acción que pueda resultar potencialmente peligrosa para las personas o que haga que el equipo no sea seguro.
- Nunca intente levantar un objeto demasiado pesado para una sola persona.

Mantener la seguridad con electricidad

> ⚠ Antes de trabajar en un chasis, asegúrese de que el cable de alimentación está desconectado.

Siga estas directrices cuando trabaje con equipo eléctrico:

- No trabaje solo si hay condiciones potencialmente peligrosas en su espacio de trabajo.
- Nunca dé por hecho que la alimentación está desconectada, compruébelo siempre.
- Busque cuidadosamente posibles riesgos en su zona de trabajo como suelos húmedos, cables de alimentación de prolongación sin toma a tierra, cables de alimentación desgastados y la falta de conexiones a tierra de seguridad.
- Si se produce un accidente eléctrico:
  - Tenga precaución, no se perjudique usted mismo.
  - Desconecte la alimentación del sistema.
  - Si es posible, envíe a otra persona para recibir asistencia médica. Si no, evalúe el estado de la víctima y, a continuación, pida ayuda.

    - Determine si el accidentado necesita respiración boca a boca o masaje cardíaco y, a continuación, realice la acción apropiada.
- Utilice el chasis según las especificaciones eléctricas y las instrucciones de uso del producto.

Evite daños por ESD

La ESD se produce cuando se manejan de manera incorrecta los componentes electrónicos, lo que puede dañar el equipo y afectar al circuito eléctrico, lo que puede dar lugar a un fallo intermitente o completo de su equipo.

Siga siempre los procedimientos de prevención de ESD cuando retire y sustituya componentes. Asegúrese de que el chasis esté eléctricamente conectado a tierra. Utilice una correa para la muñeca antiestática y asegúrese de que está en contacto con su piel. Conecte la pinza de toma a tierra a una zona sin pintura del marco del chasis para conectar a tierra de forma segura los voltajes de ESD. Para protegerse de manera adecuada frente a daños y descargas causadas por ESD, tanto la correa para la muñeca como el cable deben funcionar correctamente. Si no hay una correa de muñeca disponible, establezca una conexión a tierra usted mismo tocando una parte metálica del chasis.

Por su seguridad, compruebe periódicamente el valor de resistencia de la correa antiestática, que debe estar entre 1 y 10 megaohmios.

Entorno del sitio

Para evitar fallos en el equipo y reducir la posibilidad de que se apague por el entorno, planifique el diseño del sitio y la ubicación del equipo con cuidado. Si su equipo actual se apaga o experimenta tasas de error inusualmente altas, estas consideraciones pueden ayudarle a aislar la causa de los fallos y evitar futuros problemas.

Consideraciones de la fuente de alimentación

Al instalar el chasis, tenga en cuenta lo siguiente:

- Compruebe la alimentación en el sitio antes de instalar el chasis para garantizar que no tenga picos ni ruido. Instale un acondicionador de potencia si es necesario para asegurarse de utilizar niveles de tensión y potencia adecuados en la tensión de entrada del appliance.
- Instale una conexión a tierra adecuada para el sitio para evitar daños por rayos y subidas de potencia.
- El chasis no cuenta con un rango de funcionamiento seleccionable por el usuario. Consulte la etiqueta del chasis para conocer los requisitos de potencia de entrada correctos del appliance.

- Hay disponibles varios tipos de cables de alimentación de entrada de CA para el appliance, asegúrese de utilizar el adecuado para su sitio.
- Si utiliza fuentes de alimentación redundantes (1+1) dobles, le recomendamos que use circuitos eléctricos independientes para cada fuente de alimentación.
- Instale una fuente de alimentación continua para su sitio si es posible.

Consideraciones sobre la configuración en rack

Tenga en cuenta lo siguiente durante la planificación de la configuración en rack:

- Si monta un chasis en un rack abierto, asegúrese de que el marco del rack no bloquea los puertos de entrada o salida.
- Asegúrese de que los racks encerrados dispongan de una ventilación adecuada. Asegúrese de que el rack no se congestione excesivamente, puesto que cada chasis genera calor. Un rack encerrado debe tener laterales de ventilación y un ventilador que proporcione aire de refrigeración.
- En un rack encerrado con un ventilador de ventilación en la parte superior, el calor generado por el equipo que está cerca de la parte inferior del rack puede dirigirse hacia arriba y por los puertos de entrada del equipo de encima en el rack. Asegúrese de que se proporcione una ventilación adecuada al equipo de la parte inferior del rack.
- Los deflectores pueden ayudar a aislar el aire de salida del aire de entrada, lo cual también ayuda a guiar el aire de refrigeración en su paso por el chasis. La mejor ubicación de los deflectores depende de los patrones de aireación en el rack. Pruebe diferentes disposiciones para colocar los deflectores de forma eficaz.

Consideraciones previas a la configuración

Esta sección examina las consideraciones que debe tener en cuenta antes de instalar y configurar sus appliances de Stealthwatch. Explica dónde colocar los appliances de Steathwatch y cómo integrarlos en su red. Incluye

- **Iniciar sesión utilizando la contraseña predeterminada de CIMC**
- **Sobre los appliances de Stealthwatch**
- **Colocar sus appliances**
- **Puertos de comunicación**
- **Integrar los sensores de flujo en su red**

Iniciar sesión utilizando la contraseña predeterminada de CIMC

El Cisco Integrated Management Controller (CIMC) habilita el acceso a la configuración del servidor y a una consola del servidor virtual; además, supervisa el estado del hardware. Utilice la siguiente contraseña predeterminada para iniciar sesión en el CIMC:

`password`.

Cuando inicie sesión, cambie la contraseña predeterminada para proteger la seguridad de su red.

Sobre los appliances de Stealthwatch

Stealthwatch consta de varios appliances de hardware que recopilan, analizan y presentan información sobre su red para mejorar su rendimiento y seguridad. Esta sección describe cada appliance de Stealthwatch de la serie x210.

> Para obtener más información, consulte las hojas de especificaciones de cada appliance de Stealthwacth de la serie x210

Consola de gestión 2210 de Stealthwatch

La consola de gestión de Stealthwatch gestiona, coordina, configura y organiza los distintos componentes del sistema. El software Stealthwatch le permite acceder a la IU web de la consola desde cualquier ordenador con acceso a un navegador web. Puede acceder con facilidad a la información de red y seguridad en tiempo real sobre partes fundamentales de su empresa. Gracias a la independencia de la plataforma basada en Java, la consola de gestión de Stealthwatch permite:

- La configuración, la información y la administración centralizada de hasta 25 recopiladores de flujo de Stealthwatch
- Gráficos para visualizar el tráfico
- Análisis de detalles para la resolución de problemas
- Informes consolidados y personalizables
- Análisis de tendencias
- Supervisión del rendimiento
- Notificación inmediata de las brechas de seguridad

Recopilador de flujo 4210 y 5210 de Stealthwatch

El recopilador de flujo de Stealthwatch incluye datos cFlow, J-Flow, Packeteer 2, NetStream e IPFIX para ofrecer protección de red basada en el comportamiento.

El recopilador de flujo agrega datos de comportamiento de la red de alta velocidad procedentes de varias redes o segmentos de red para posibilitar una protección integral y mejorar el rendimiento en redes situadas en diversas ubicaciones.

> A medida que el recopilador de flujo recibe datos, identifica ataques conocidos o desconocidos, el uso indebido interno y dispositivos de red mal configurados independientemente de si hay fragmentación o cifrado de paquetes. Una vez que Stealthwatch identifica el comportamiento, el sistema puede llevar a cabo cualquier medida que haya configurado, si es que la hay, para dicho tipo de comportamiento.

Sensor de flujo 1210, 3210 y 4210 de Stealthwatch

El sensor de flujo de Stealthwatch es un appliance de red que funciona de forma similar a la de los habituales appliances de captura de paquetes o IDS que se conecta en un analizador de puerto de switch (SPAN), un puerto de reflejo o un puerto de acceso de prueba (TAP) de Ethernet. El sensor de flujo aumenta la visibilidad en las siguientes áreas de red:

- Donde NetFlow no está disponible.
- Donde NetFlow está disponible pero desea obtener una mayor visibilidad de los indicadores de rendimiento y datos del paquete.

Al dirigir el sensor de flujo hacia cualquier recopilador de flujo compatible con NetFlow v9, obtendrá útiles estadísticas del tráfico detalladas de NetFlow. Cuando se combina con el recopilador de flujo de Stealthwatch, el sensor de flujo también ofrece una visión detallada de los indicadores de rendimiento y de comportamiento. Estos indicadores de

rendimiento del flujo ofrecen una visión de latencia de recorrido de ida y vuelta introducida por la red o por la aplicación del lado servidor.

Ya que el sensor de flujo consta de visibilidad a nivel del paquete, puede calcular el tiempo de ida y vuelta (RTT), el tiempo de respuesta del servidor (SRT) y la pérdida de paquetes para sesiones TCP. Incluye todos estos campos adicionales en los registros de NetFlow que envía al recopilador de flujo.

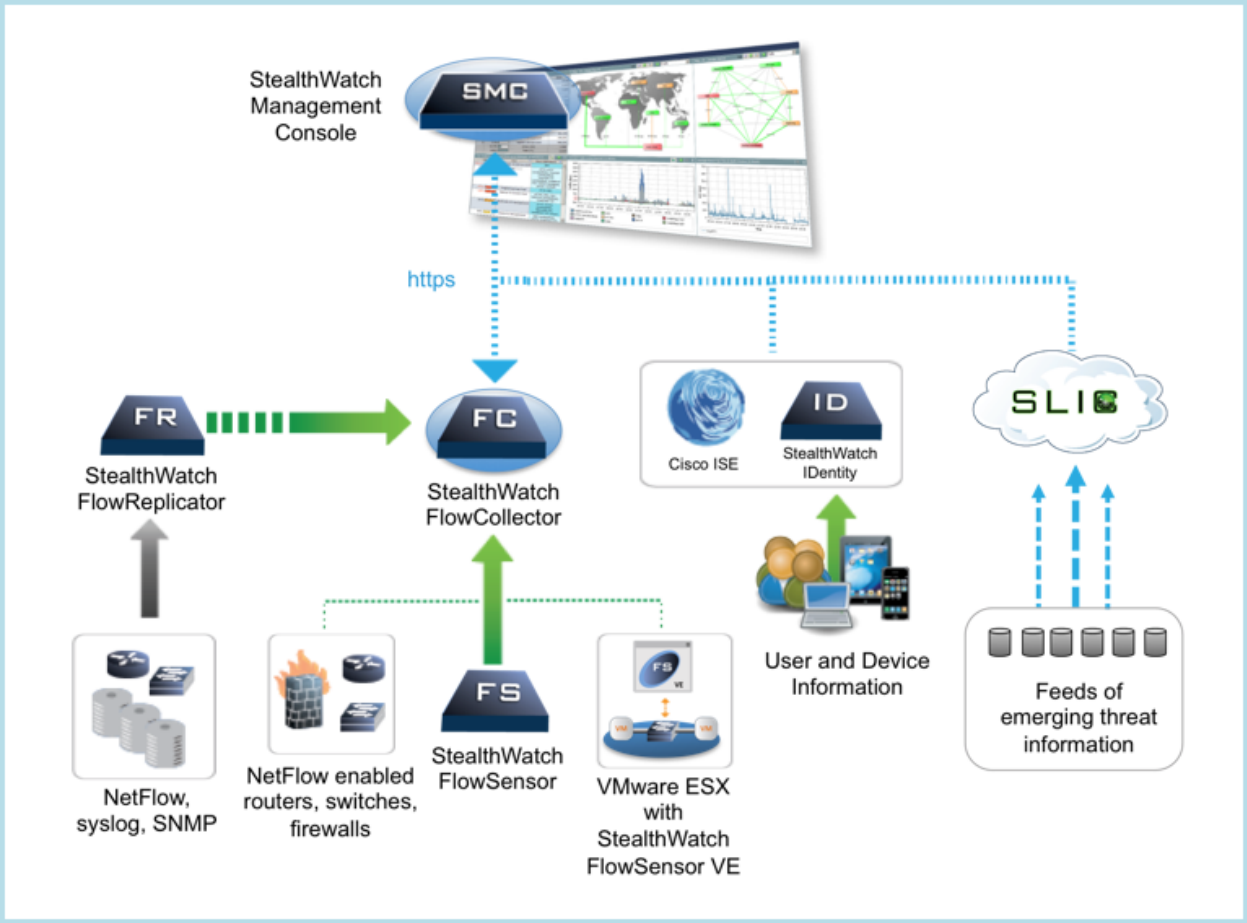
UDP Director 2210 de Stealthwatch

El UDP Director de Stealthwatch es un replicador del paquete de UDP de gran velocidad y alto rendimiento. El UDP Director es de gran utilidad para la redistribución de las trampas de NetFlow, sFlow, syslog o del Protocolo simple de administración de red (SNMP) en varios recopiladores. Puede recibir datos de cualquier aplicación UDP sin conexión y, a continuación, los retransmite a varios destinos y los duplica si así se requiere.

Si utiliza la configuración (conmutación por error) de alta disponibilidad (HA) del UDP Director, debe conectar dos appliances de UDP Director con cables cruzados. Para obtener instrucciones específicas, consulte **Conexión de su appliance a la red**.

Colocar sus appliances

Tal y como se muestra en la siguiente figura, puede implementar de forma estratégica los appliances de Stealthwatch para ofrecer una cobertura óptima de los segmentos de la red claves en la red, ya sea en la red interna, en el perímetro, o en el DMZ.



Colocar la consola de gestión de Stealthwatch

Como el dispositivo de administración, instale la consola de gestión de Stealthwatch en una ubicación de su red que sea accesible para todos los dispositivos que le envíen datos.

Si tiene un par de conmutación por error de las consolas de gestión de Stealthwatch, le recomendamos instalar las consolas primaria y secundaria en ubicaciones físicas separadas. Esta estrategia fomentará un esfuerzo de recuperación de desastres si es necesario.

Colocar el recopilador de flujo de Stealthwatch

Como dispositivo de supervisión y recopilación, el recopilador de flujo de Stealthwatch se debe instalar en una ubicación en su red que sea accesible para los dispositivos de NetWflow o sFlow que envían datos a un recopilador de flujo, así como para cualquier dispositivo que desee utilizar para acceder a la interfaz de administración.

Cuando coloque un recopilador de flujo fuera de un firewall, le recomendamos que desconecte la configuración **Aceptar tráfico de cualquier exportador**.

Colocar el sensor de flujo de Stealthwatch

Como dispositivo de supervisión pasivo, el sensor de flujo de Stealthwatch puede establecer varios puntos en su red para observar y registrar la actividad de IP, de modo que se proteja la integridad de la red y se detecten las brechas de seguridad. Las características del sensor de flujo integradas en los sistemas de administración basados en la web que facilitan la gestión y la administración ya sea remota o centralizada.

El appliance del sensor de flujo es más efectivo cuando se ubica en segmentos cruciales de su red corporativa de la siguiente forma:

- Dentro de su firewall para supervisar el tráfico y determinar si se ha producido una brecha de seguridad
- Fuera de su firewall, monitorizando el flujo de tráfico para analizar quién está amenazando su firewall
- En los segmentos sensibles de su red ofreciendo así protección contra empleados descontentos o hackers que tienen acceso raíz
- En ubicaciones remotas de la oficina que constituyan extensiones de la red vulnerables
- En su red empresarial para la gestión de uso del protocolo (por ejemplo, en su subred de servicios de transacción para determinar si un hacker está ejecutando Telnet o FTP y poniendo en peligro los datos financieros de sus clientes)

Colocar el UDP Director de Stealthwatch

El único requisito para la ubicación de UDP Director de Stealthwatch es que tenga una ruta de comunicación libre para el resto de sus appliances de Stealthwatch.

Configurar su firewall para las comunicaciones

Para que los appliances se puedan comunicar de forma correcta, debe configurar la red de forma que los firewall o las listas de control de acceso no bloqueen las conexiones requeridas. Utilice los diagramas y tablas mostrados en esta sección para configurar su red de forma que los appliances puedan comunicarse a través de la red.

Póngase en contacto con su administrador de red para garantizar que los siguientes puertos están abiertos y no tienen acceso restringido:

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393

- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Puertos de comunicación

La siguiente tabla muestra cómo se utilizan los puertos en Stealthwatch:

Desde (cliente)	A (servidor)	Puerto	Protocolo
PC del usuario administrador	Todos los appliances	TCP/443	HTTPS
Todos los appliances	Fuente de tiempo de red	UDP/123	NTP
Active Directory	Consola de gestión de Stealthwatch	TCP/389, UDP/389	LDAP
AnyConnect	Terminal Concentrador	UDP/2055	NetFlow
Cisco ISE	Consola de gestión de Stealthwatch	TCP/443	HTTPS
Cisco ISE	Consola de gestión de Stealthwatch	TCP/5222	XMPP
Concentrador de terminal	Recopilador de flujo	UDP/2055	NetFlow
Fuentes de registro externo	Consola de gestión de Stealthwatch	UDP/514	SYSLOG
Recopilador de flujo	Consola de gestión de Stealthwatch	TCP/443	HTTPS
SLIC	Consola de gestión de Stealthwatch	TCP/443 o conexión por proxy	HTTPS
UDP Director	Recopilador de flujo: sFlow	UDP/6343	sFlow
UDP Director	Recopilador de flujo: NetFlow	UDP/2055*	NetFlow
UDP Director	Sistemas de gestión de eventos de terceros	UDP/514	SYSLOG

Desde (cliente)	A (servidor)	Puerto	Protocolo
Sensor de flujo	Consola de gestión de Stealth-watch	TCP/443	HTTPS
Sensor de flujo	Recopilador de flujo: NetFlow	UDP/2055	NetFlow
Identidad	Consola de gestión de Stealth-watch	TCP/2393	SSL
Exportadores de NetFlow	Recopilador de flujo: NetFlow	UDP/2055*	NetFlow
Exportadores de sFlow	Recopilador de flujo: sFlow	UDP/6343*	sFlow
Consola de gestión de Stealthwatch	Cisco ISE	TCP/443	HTTPS
Consola de gestión de Stealthwatch	DNS	UDP/53	DNS
Consola de gestión de Stealthwatch	Recopilador de flujo	TCP/443	HTTPS
Consola de gestión de Stealthwatch	Sensor de flujo	TCP/443	HTTPS
Consola de gestión de Stealthwatch	Identidad	TCP/2393	SSL
Consola de gestión de Stealthwatch	Exportadores de flujo	UDP/161	SNMP
Consola de gestión de Stealthwatch	Concentrador de terminal	UDP.2055	HTTPS
PC del usuario	Consola de gestión de Stealth-watch	TCP/443	HTTPS

*Este es el puerto predeterminado pero cualquier puerto UDP se puede configurar en el exportador.

La siguiente tabla es para configuraciones opcionales determinadas por sus necesidades de red:

De (cliente)	A (servidor)	Puerto	Protocolo
Todos los dispositivos	PC del usuario	TCP/22	SSH
Consola de gestión de Stealthwatch	Gestión de eventos de terceros	UDP/162	Trampa SNMP
Consola de gestión de Stealthwatch	Gestión de eventos de terceros	UDP/514	SYSLOG
Consola de gestión de Stealthwatch	Gateway de correo electrónico	TCP/25	SMTP
Consola de gestión de Stealthwatch	SLIC	TCP/443	SSL
PC del usuario	Todos los dispositivos	TCP/22	SSH

El siguiente diagrama muestra las distintas conexiones que Stealthwatch utiliza. Los puertos marcados como opcionales son los que se pueden utilizar para sus propias necesidades de red.

Integrar los sensores de flujo en su red

El sensor de flujo de Stealthwatch es versátil para integrarlo con una amplia gama de topologías de red, tecnologías y componentes. Ya que no se pueden tratar aquí todas las configuraciones de red, puede que los ejemplos le ayuden a determinar la configuración que mejor satisfaga sus necesidades.

Antes de instalar el sensor de flujo, debe tomar varias decisiones sobre su red y cómo desea supervisarla. Asegúrese de analizar tanto su topología de red como sus necesidades específicas de supervisión. Es recomendable que conecte un sensor de flujo de forma que reciba transmisiones de red entrantes y salientes de la red supervisada y, si lo desea, también reciba transmisiones de red internas.

En las siguientes secciones se explica cómo integrar un appliance de sensor de flujo de Stealthwatch en su red utilizando los siguientes dispositivos de red Ethernet:

- **TAP**
- **Puertos SPAN**

TAP

Cuando se coloca un puerto de acceso de prueba (TAP) en línea con una conexión de red, repite la conexión en un puerto o en varios puertos independientes. Por ejemplo, un TAP de Ethernet colocado en línea con un cable Ethernet repetirá cada dirección de transmisión a puertos independientes. Por lo tanto, emplear un TAP es la forma más fiable de utilizar el sensor de flujo. El tipo de TAP que utilice depende de su red.

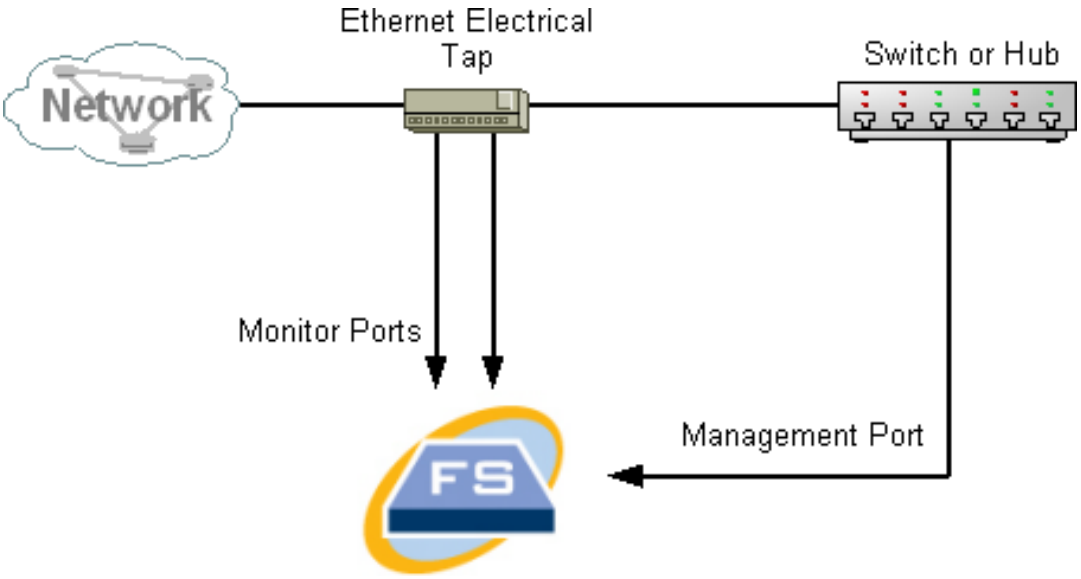
Esta sección explica las siguientes formas de utilizar TAP:

- **Utilizar TAP eléctricos**
- **Utilizar TAP ópticos**
- **Utilizar TAP fuera de su firewall**
- **Colocar el sensor de flujo dentro de su firewall**

En una red que utilice TAP, el sensor de flujo solo puede recopilar datos de supervisión del rendimiento si está conectado a un TAP de agregación que capte el tráfico entrante y saliente. Si el sensor de flujo está conectado a un TAP unidireccional que capta solo una dirección del tráfico en cada puerto, el sensor de flujo no recopilará los datos de supervisión del rendimiento.

Utilizar TAP eléctricos

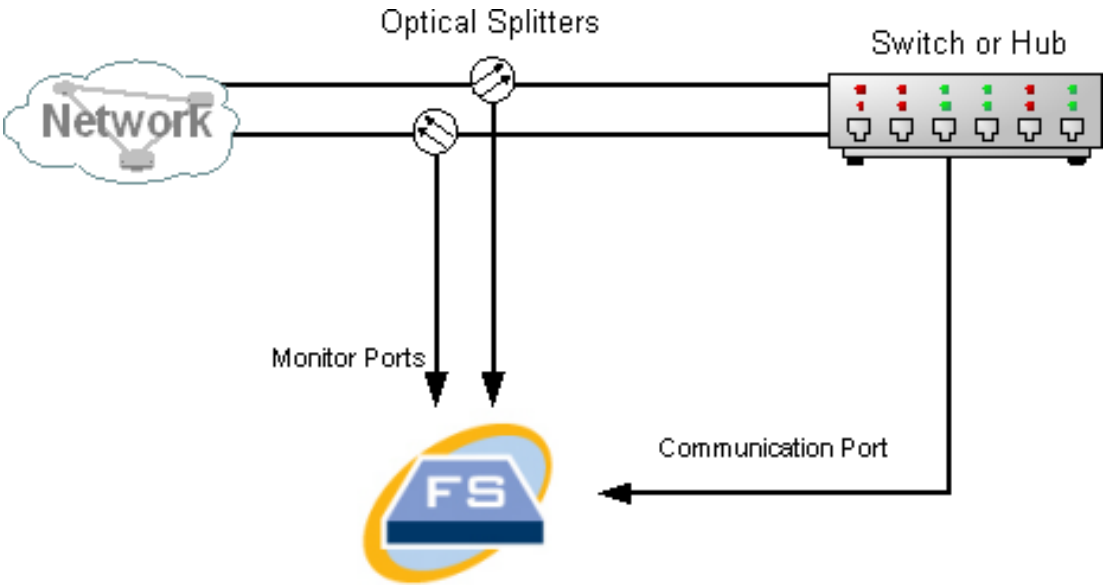
En el siguiente ejemplo, el sensor de flujo está conectado a un TAP eléctrico de Ethernet. Para ello, conecte los dos puertos TAP a los puertos de supervisión del sensor de flujo 1 y 2.



Utilizar TAP ópticos

Utilice dos divisores para sistemas de fibra óptica. Coloque un divisor de cable de fibra óptica en línea con cada dirección de transmisión para repetir la señal óptica de una dirección de transmisión.

En el siguiente ejemplo, el sensor de flujo se conecta a una red basada en fibra óptica. Para ello, conecte las salidas de los divisores a los puertos de supervisión del sensor de flujo 1 y 2.



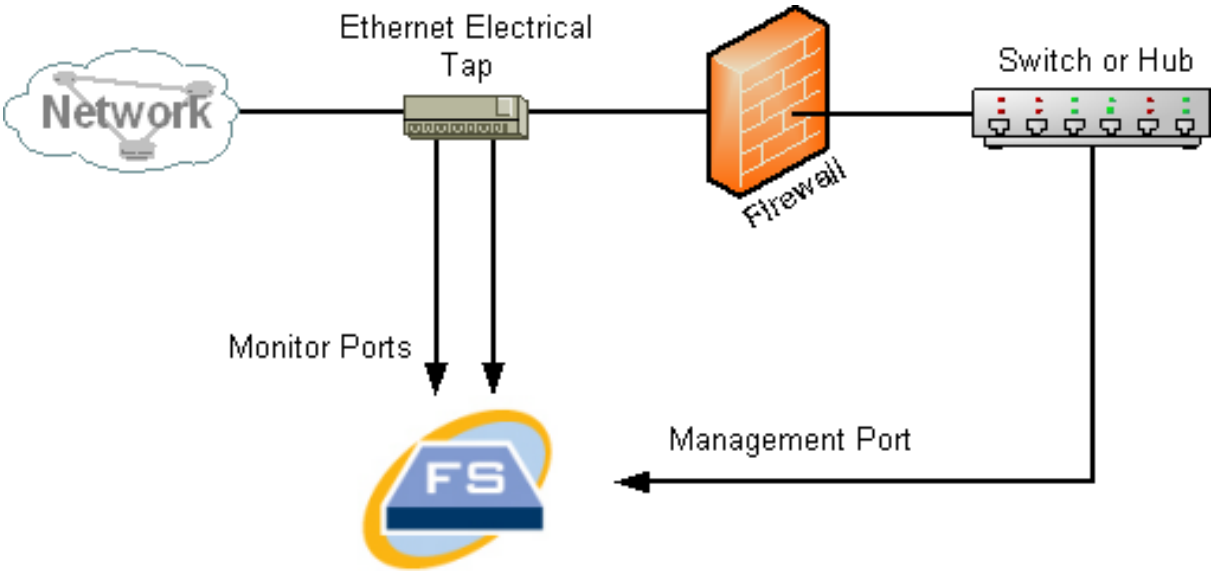
Si la conexión entre las redes supervisadas es una conexión opcional, el sensor de flujo se conecta a dos divisores ópticos. El puerto de gestión se conecta al switch de la red supervisada o a otro switch o hub.

Utilizar TAP fuera de su firewall

Para que el tráfico de supervisión del sensor de flujo se sitúe entre su firewall y otras redes, conecte el puerto de gestión de Stealthwatch a un switch o puerto fuera del firewall.

Le recomendamos encarecidamente que utilice un TAP para esta conexión de forma que el fallo del dispositivo no haga caer su red por completo.

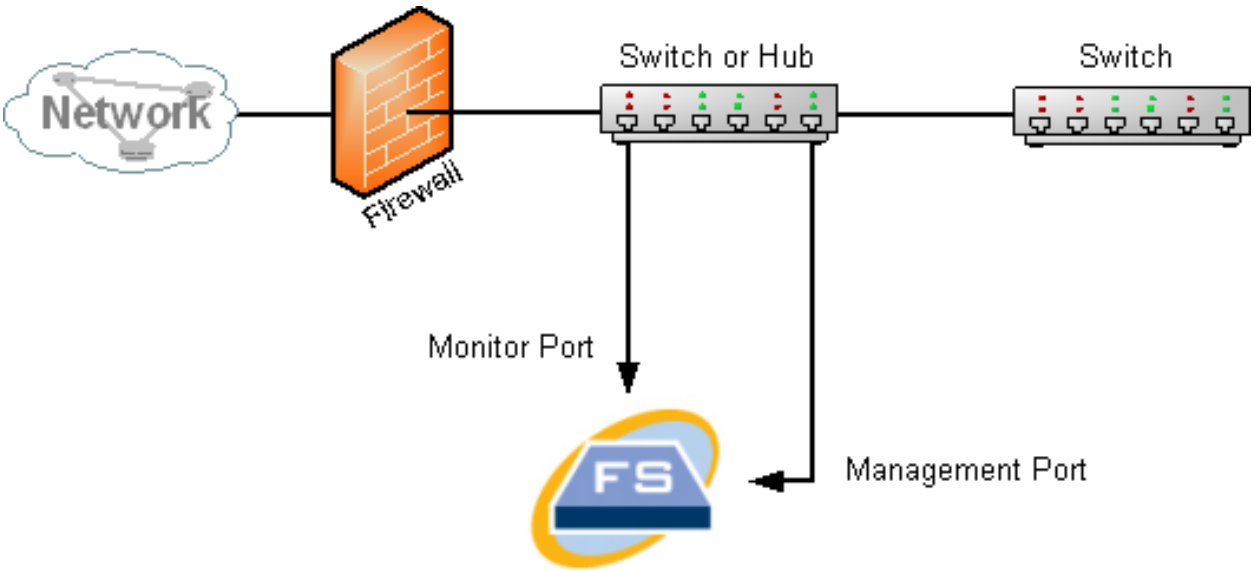
En el siguiente ejemplo se muestra el uso de un TAP eléctrico de Ethernet. El puerto de administración debe estar conectado al switch o hub de la red supervisada. Esta configuración es similar a la configuración que supervisa el tráfico de entrada y de salida de su red.



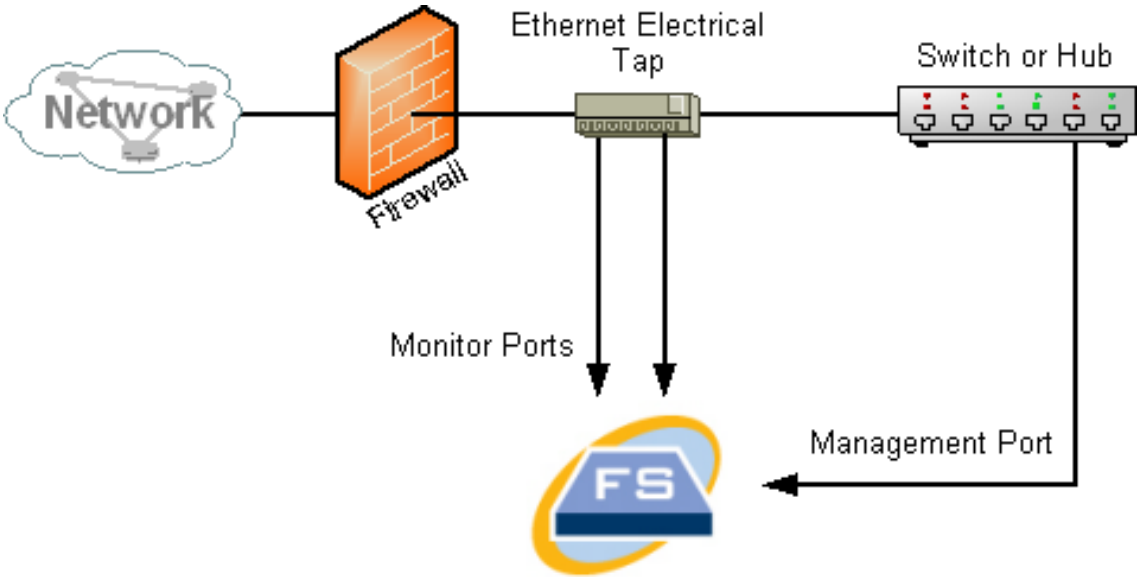
Si su firewall está realizando una traducción de direcciones de red (NAT) solo puede ver las direcciones que se encuentren en el firewall.

Colocar el sensor de flujo dentro de su firewall

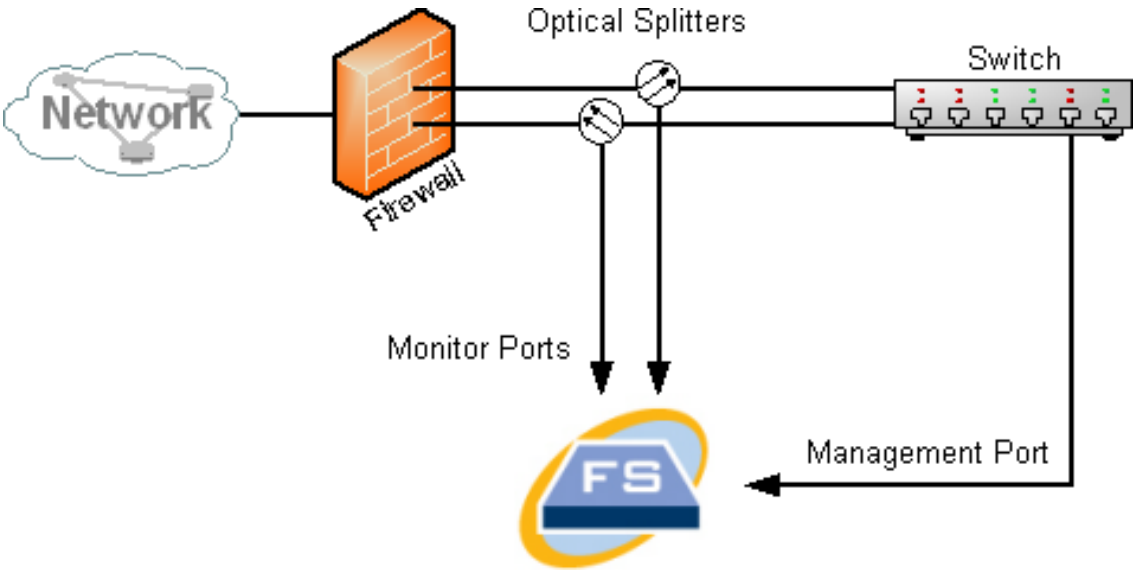
Para supervisar el tráfico entre redes internas y un firewall, el sensor de flujo debe tener acceso a todo el tráfico entre el firewall y las redes internas. Puede lograrlo al configurar un puerto de reflejo para que duplique la conexión al firewall en el switch principal. Asegúrese de que el puerto 1 de supervisión del sensor de flujo está conectado al puerto de reflejo tal y como se muestra en la siguiente imagen:



Para supervisar el tráfico dentro de su firewall usando un TAP, inserte el TAP o el divisor óptico entre su firewall y el switch principal o hub. A continuación se muestra una configuración de TAP.



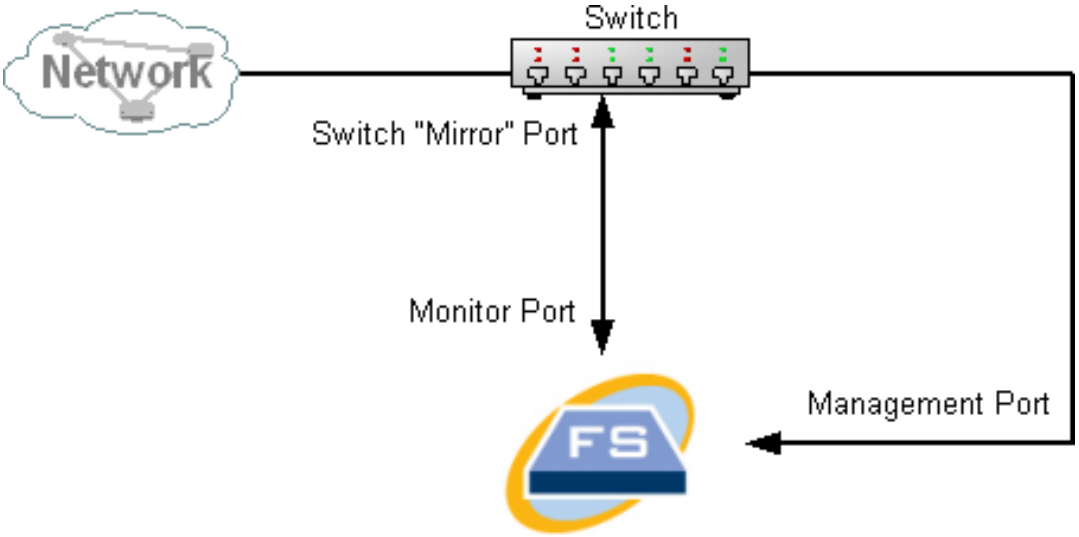
A continuación se muestra una configuración de divisor óptico.



Puertos SPAN

También puede conectar el sensor de flujo a un switch. Sin embargo, debido a que su switch no repite todo el tráfico en cada puerto, el sensor de flujo no rendirá de forma adecuada salvo que el switch pueda repetir los paquetes transmitidos a uno o más puertos de switch y desde ellos. Este tipo de puerto de switch en algunas ocasiones se llama puerto de reflejo o analizador de puerto de switch (SPAN).

La siguiente ilustración muestra cómo puede conseguir dicha configuración al conectar su red al sensor de flujo de Stealthwatch a través del puerto de gestión.



En esta configuración, debe configurar un puerto de switch (también llamado puerto de reflejo) para repetir todo el tráfico de entrada y de salida del host de interés para el

puerto de reflejo. El puerto 1 de supervisión del sensor de flujo se debe conectar a este puerto de reflejo. Esto permite que el sensor de flujo supervise el tráfico de entrada y de salida de la red de interés y a otras redes. En este caso, una red podría estar constituida por algunos o todos los host conectados al switch.

Una forma habitual de configurar redes en un switch es dividirlas en redes de área local virtuales (VLAN), que son conexiones de host lógicas en lugar de físicas. Si el puerto de reflejo está configurado para duplicar todos los puertos en una VLAN o switch, el sensor de flujo puede supervisar todo el tráfico de entrada y de salida y en la red de interés, así como otras redes.

En todos los casos, le recomendamos que consulte la documentación del fabricante de su switch para determinar cómo configurar el puerto de reflejo de switch y lo que el tráfico repetirá en el puerto de reflejo.

Instalación

Este apartado abarca la instalación de sus appliances en su entorno. Incluye

- **Montaje de su appliance**
- **Conexión de su appliance a la red**
- **Conexión a su appliance**
- **Cambio de información predeterminada**

Montaje de su appliance

Puede montar appliances de Stealthwatch directamente en un rack o armario estándar de 19", cualquier otro armario adecuado o en una superficie plana. Al montar un appliance en un rack o en un armario, siga las instrucciones que se incluyen en los kits de montaje en raíles. Al determinar dónde colocar un appliance, asegúrese de que la separación en los paneles frontales y traseros es la siguiente:

- Los indicadores del panel frontal se pueden leer con facilidad
- El acceso a los puertos en el panel trasero es suficiente para conectar el cableado sin restricciones
- La entrada de alimentación del panel trasero está al alcance de una fuente de alimentación de CA acondicionada.
- El flujo de aire en torno al appliance y a través de los orificios de ventilación no se encuentra obstaculizado.

Hardware incluido en el appliance

El siguiente hardware se incluye en appliances de Stealthwatch:

- Cable de alimentación de CA
- Llaves de acceso (para la placa frontal)
- Kit de raíles para el montaje en rack o agarraderas de montaje para appliances más pequeños
- Un cable SFP de 10 GB para el recopilador de flujo 5210

Hardware adicional necesario

Debe proporcionar el siguiente hardware adicional necesario:

- Tornillo de montaje para un rack estándar de 19"
- Fuente de alimentación ininterrumpida (UPS) para cada appliance que instale
- Para configurar de forma local (opcional), utilice uno de los siguientes métodos:
  - Un ordenador portátil con un cable de vídeo y un cable USB (para el teclado)
  - Un monitor de vídeo con un cable de vídeo y un teclado con un cable USB

Conexión de su appliance a la red

Utilice el mismo procedimiento para conectar cada appliance a la red. La única diferencia para la conexión es el tipo de appliance que tiene.

Para obtener información detallada sobre las especificaciones de cada appliance, consulte las hojas de especificaciones de Stealthwatch.

> Todo el hardware de Cisco x210 utiliza la misma plataforma de UCS, UCSC-C220-M5SX, excepto en el caso del recopilador de flujo de 5120 DB, que utiliza UCSC-C240-M5SX. Las variaciones en los appliances se encuentran en las tarjetas NIC, el procesador, la memoria, el almacenamiento y RAID.

> El recopilador de flujo 5210 consta de dos servidores conectados (motor y base de datos) para que funcionen como un solo appliance. Por este motivo, la instalación cambia ligeramente respecto a otros appliances. En primer lugar, conéctelos directamente mediante un cable cruzado de 10 G SFP+ de conexión directa. A continuación, conéctese a la red.

Para conectar su appliance a su red:

1. Conecte un cable de Ethernet al puerto de gestión, en la parte trasera del appliance.
2. Conecte al menos un puerto de supervisión para el sensor de flujo y los UDP Director.

   Para la HA de UDP Director, conecte los dos UDP Director mediante cables cruzados. Conecte el puerto eth2 de un UDP Director al puerto eth2 del segundo UDP Director. De manera similar, conecte el puerto de eth3 de cada UDP Director con un segundo cable cruzado. Puede ser el cable de fibra o de cobre.

   Asegúrese de tener en cuenta la etiqueta de Ethernet (eth2, eth3, etc.) para cada puerto. Estas etiquetas corresponden a las interfaces de red (eth2, eth3, etc.) que

se muestran y se pueden configurar en la página de inicio de la interfaz de administración del appliance.

3. Conecte el otro extremo de los cables Ethernet a su switch de red.
4. Conecte los cables de alimentación a la fuente de alimentación. Algunos appliances tienen dos conexiones de alimentación: fuente de alimentación 1 y fuente de alimentación 2.

Conexión a su appliance

Esta sección describe cómo conectarse a su appliance para cambiar las contraseñas predeterminadas del usuario.

Puede conectarse al appliance en uno de estos dos modos:

- con un teclado y un monitor
- con un ordenador portátil (y un emulador del terminal)

El SSH está desactivado para los nuevos appliances. Debe iniciar sesión en la interfaz web de administración del appliance para activarlo.

Conexión con un teclado y un monitor

Para configurar la dirección IP de forma local, siga estos pasos:

1. Conecte el cable de alimentación al appliance.
2. Pulse el botón de alimentación para encender el appliance. Espere a que haya terminado de arrancar por completo. No interrumpa el proceso de arranque.

> Puede que tenga que quitar el panel frontal para que llegue la alimentación.
>
> Los ventiladores de la fuente de alimentación se conectan en algunos modelos cuando el sistema no está encendido. Compruebe que el LED en el panel frontal está encendido.
>
> Asegúrese de conectar el appliance a una fuente de alimentación ininterrumpida (UPS). La fuente de alimentación precisa alimentación o de lo contrario el sistema mostrará un error.

3. Conecte el teclado:

- Si dispone de un teclado estándar, conéctelo al conector estándar de teclado.
- Si dispone de un teclado USB, conéctelo a un conector USB.

4. Conecte el cable de vídeo al conector de vídeo. Aparecerá la indicación de inicio de sesión.
5. Continúe con la sección, **Cambio de información predeterminada**.

Conexión con un ordenador portátil

También puede conectarse al appliance con un ordenador portátil que tenga un emulador del terminal.

Para conectarse a un appliance con un ordenador portátil:

1. Conecte su ordenador portátil al appliance utilizando uno de los siguientes métodos:
   - Conecte un cable RS232 del conector de puertos en serie (DB8) en su ordenador portátil al puerto de consola en el appliance.
   - Conecte un cable cruzado del puerto Ethernet en su ordenador portátil al puerto de gestión en el appliance.
2. Conecte el cable de alimentación al appliance.
3. Pulse el botón de alimentación para encender el appliance. Espere a que haya terminado de arrancar por completo. No interrumpa el proceso de arranque.

   > Puede que tenga que quitar el panel frontal para que llegue la alimentación.
   >
   > Los ventiladores de la fuente de alimentación se conectan en algunos modelos cuando el sistema no está encendido. Compruebe que el LED en el panel frontal está encendido. Asegúrese de conectar el appliance a una fuente de alimentación ininterrumpida (UPS). La fuente de alimentación precisa alimentación o de lo contrario el sistema mostrará un error.

4. En el ordenador portátil, establezca una conexión con el appliance.

   Puede utilizar cualquier emulador del terminal para comunicarse con el appliance.

5. Aplique los siguientes ajustes:
   - BPS: 115200
   - Bits de datos: 8
   - Bit de parada: 1
   - Paridad: ninguna
   - Control de flujo: ninguno

   Se muestran la pantalla y la indicación de inicio de sesión.

6. Continúe con la siguiente sección, **Cambio de información predeterminada**.

Cambio de información predeterminada

Después de que se haya conectado al appliance, configure las direcciones IP y cambie las contraseñas del usuario.

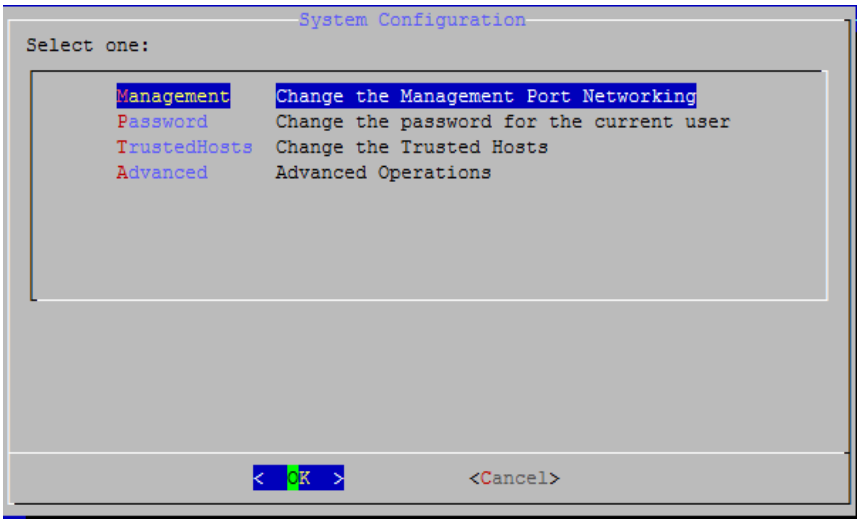
Cambio de las direcciones IP predeterminadas

Los appliances ya tienen direcciones IP predeterminadas pero configúrelas para su red.

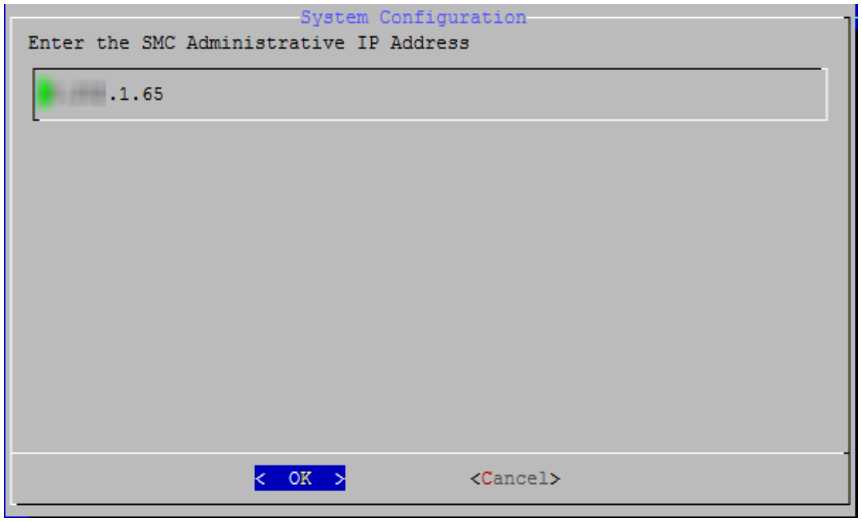
1. Inicie sesión en el programa de configuración del sistema:

   - Escriba **sysadmin**y, a continuación, pulse **Intro**.
   - Cuando aparezca la indicación de la contraseña, escriba **lan1copey**, a continuación, pulse **Intro**.
   - En la siguiente indicación escriba **SystemConfig**y, a continuación, pulse **Intro**.

     Se abrirá el menú de configuración de sistema.

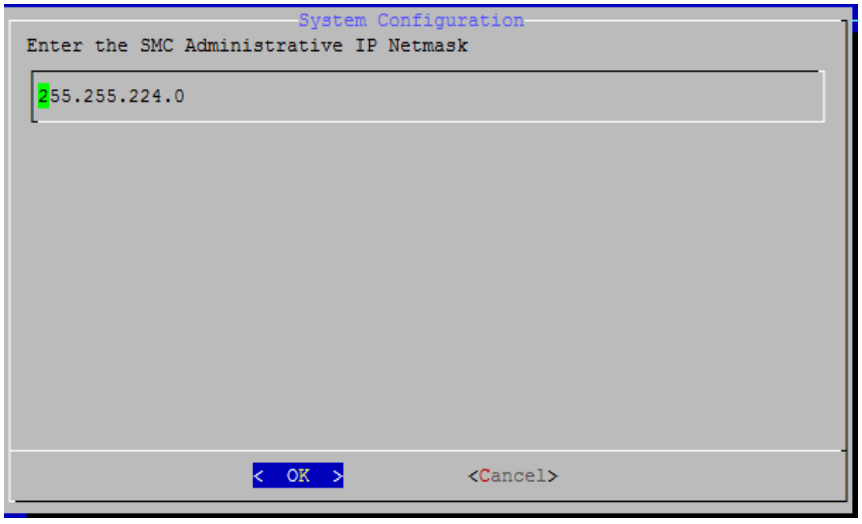


2. Seleccione **Management** (Gestión) y, a continuación, pulse **Intro**. Se abre la página de dirección de IP.



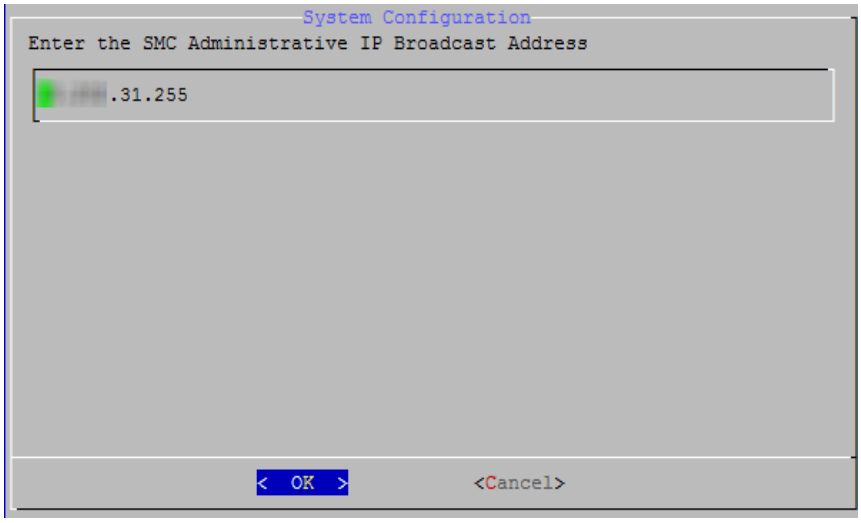
3. Escriba una nueva dirección IP basada en su entorno. Seleccione **OK** (Aceptar) y, a continuación, pulse **Intro** para continuar.

   Se abre la página de la máscara de red de IP con el valor predeterminado.



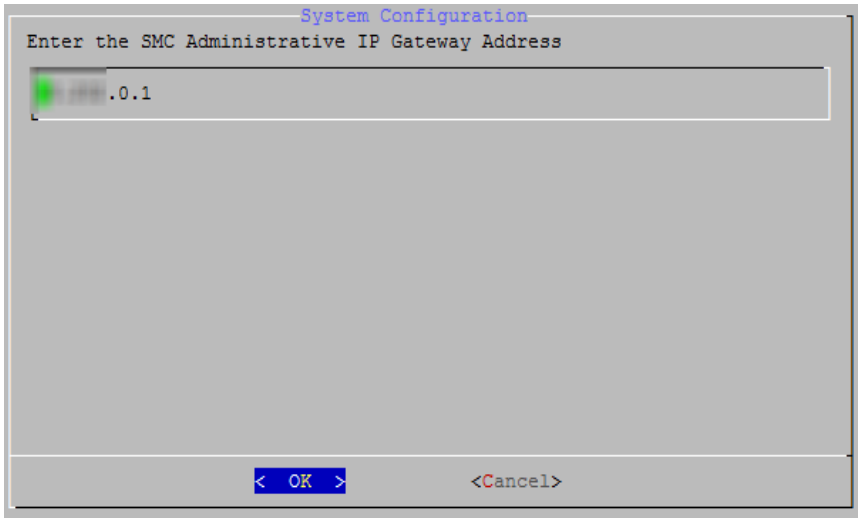
4. Acepte el valor predeterminado o introduzca una nueva dirección IP de máscara de red basada en su entorno. Seleccione **OK** (Aceptar) y, a continuación, pulse **Intro** para continuar.

Se abre la página de dirección de difusión.



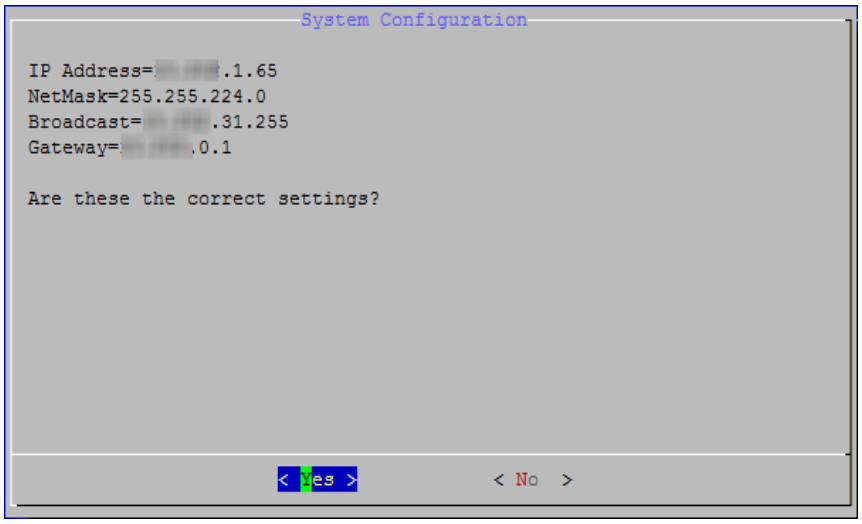
5. Acepte el valor predeterminado o introduzca uno nuevo basado en su entorno. Seleccione **Aceptar** y, a continuación, pulse **Intro** para continuar.

   Se abrirá la página de la dirección de gateway con la dirección IP del servidor de gateway predeterminada.



6. Acepte el valor predeterminado o introduzca uno nuevo basado en su entorno. Seleccione **OK** (Aceptar) y, a continuación, pulse **Intro** para continuar.

Se abre la página de confirmación.



7. Revise la información ¿Son correctos los ajustes?

- En caso afirmativo, seleccione **Yes** (Sí) y, a continuación, pulse **Intro** para continuar. El sistema se reinicia e implementa los cambios. Una vez que se complete, se abre la página de inicio de sesión.
- En caso negativo, seleccione **No** para realizar correcciones. Se abre una página de dirección IP para que pueda introducir sus cambios. Después de que se realicen los cambios y acepte la configuración, se abre la página de reinicio. Pulse **Intro** para implementar los cambios.***No recibí una página con un mensaje de reinicio.***

8. Continúe con la siguiente sección,**Cambio de la contraseña del usuario del administrador de sistemas**.

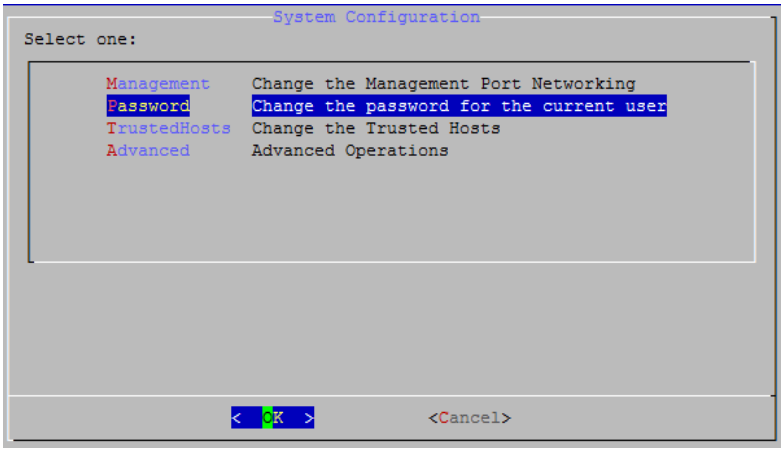
Cambio de la contraseña del usuario del administrador de sistemas

Para garantizar que la red es segura, cambie la contraseña predeterminada del administrador de sistemas para los appliances.

Asegúrese de que ha iniciado sesión como **sysadmin** para comenzar a este procedimiento.

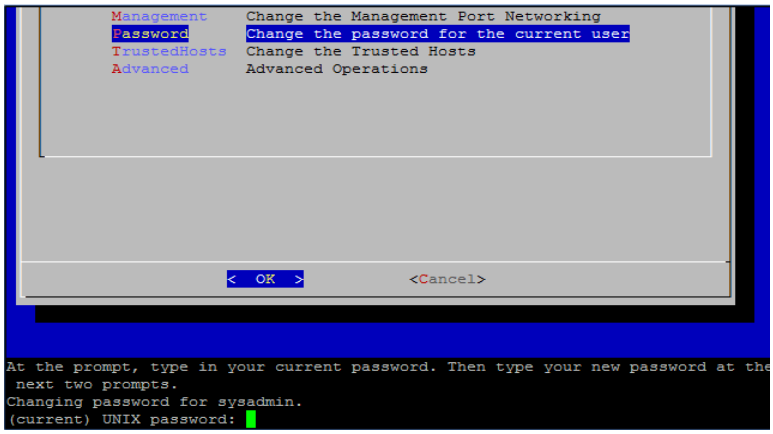
Para cambiar la contraseña del administrador de sistemas:

1. En el menú System Configuration (Configuración del sistema), seleccione **Password** (Contraseña) y pulse **Intro**.



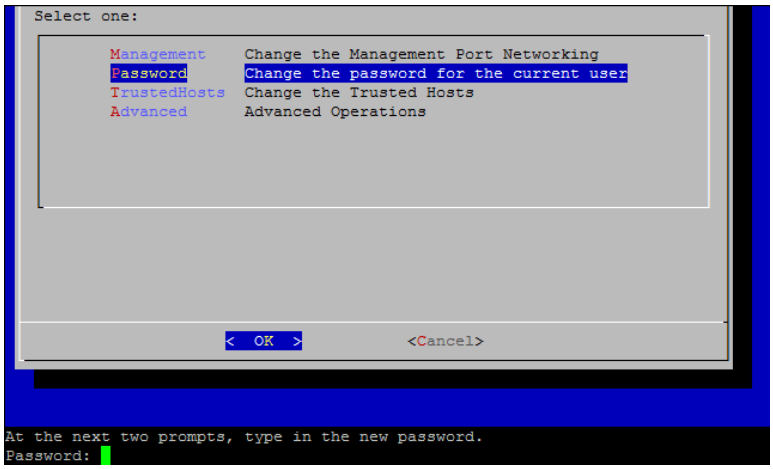
   Si cambia la lista de hosts de confianza de los valores predeterminados, asegúrese de que se incluyen todos los appliances de Stealthwatch de confianza en la lista de hosts de confianza para cada appliance de Stealthwatch en su implementación. De lo contrario, los appliances no podrán comunicarse entre sí.

   Aparecerá una indicación para la contraseña actual bajo el menú.



2. Escriba la contraseña actual y, a continuación, pulse **Intro**.

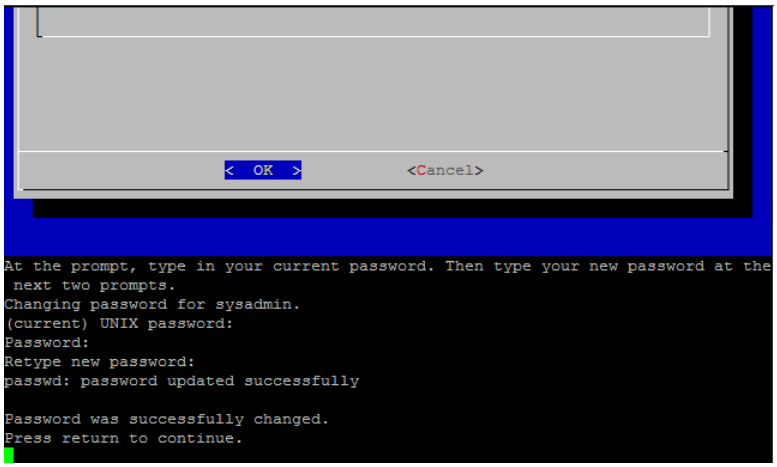
   Aparecerá la indicación para una contraseña nueva.



3. Escriba la contraseña nueva y, a continuación, pulse **Intro**.

   La contraseña debe tener entre 8 y 30 caracteres alfanuméricos sin espacios. También puede utilizar los siguientes caracteres especiales: $.~!@#%_=?:,{}()

4. Escriba la contraseña de nuevo y, a continuación, pulse **Intro**.

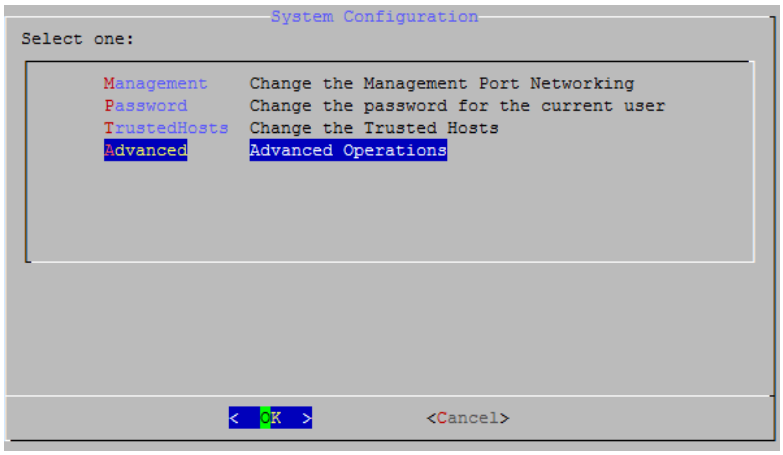


5. Cuando se acepte su contraseña, pulse **Intro** de nuevo para volver al menú System Configuration (Configuración del sistema).
6. Continúe con la siguiente sección, **Cambio de la contraseña del usuario raíz**.

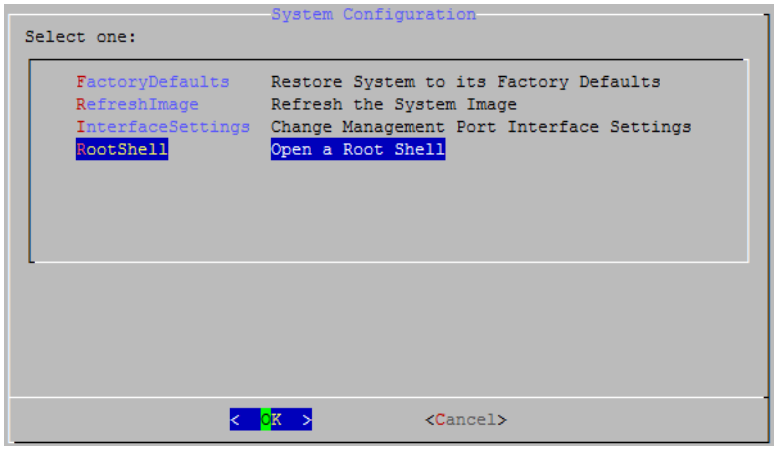
Cambio de la contraseña del usuario raíz

Después de cambiar la contraseña de usuario del administrador de sistemas, cambie la contraseña predeterminada del usuario raíz para proteger más la seguridad de su red.

1. Vaya al shell de raíz.

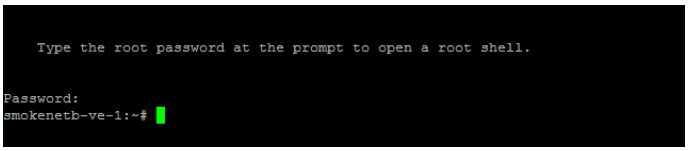


2. En el menú System Configuration (Configuración del sistema), seleccione **Advanced** (Avanzada) y, a continuación, pulse **Intro**. Aparecerá el menú Advanced (Avanzada).

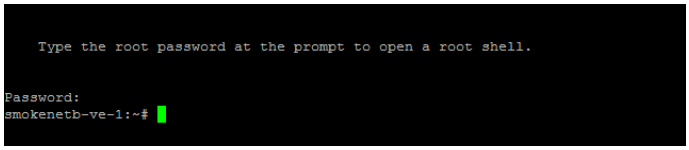


3. Seleccione **RootShell**y, a continuación, pulse **Intro**.

   Aparece una indicación para la contraseña raíz.



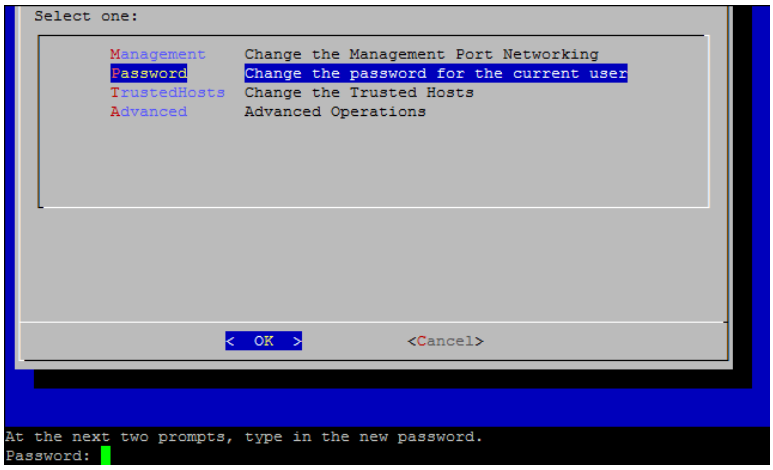
4. Escriba la contraseña raíz y, a continuación, pulse **Intro**. Aparece la indicación de shell de raíz.



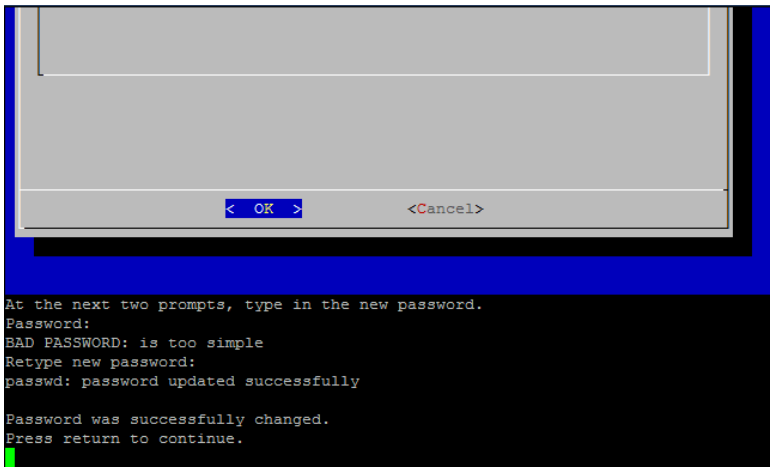
5. Escriba **SystemConfig** y, a continuación, pulse **Intro**.

   Esto le devuelve al menú System Configuration (Configuración del sistema) para que pueda cambiar la contraseña raíz.

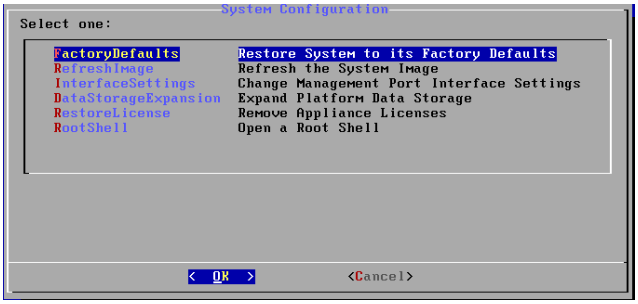
6. Seleccione **Password** (Contraseña) y, a continuación, pulse **Intro**. La indicación de contraseña aparece debajo del menú.



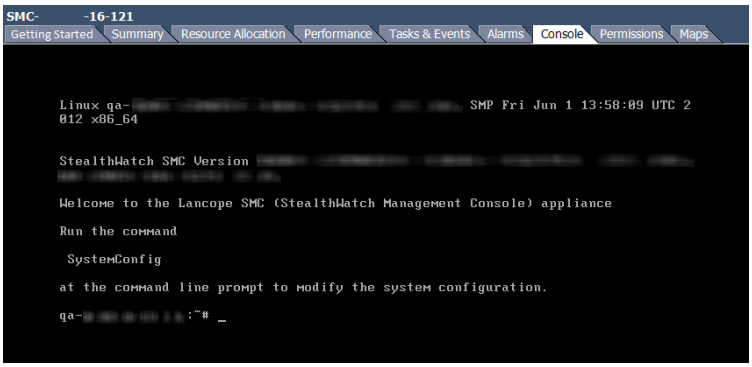
7. Escriba la nueva contraseña raíz y, a continuación, pulse **Intro**. Aparece una segunda indicación.



8. Vuelva a escribir la nueva contraseña raíz y, a continuación, pulse **Intro**.
9. Cuando el cambio de contraseña se realice correctamente, pulse **Intro**. Ha cambiado sus contraseñas raíz y de administrador de sistemas predeterminadas. Esto le devuelve al menú System Configuration Console (Consola de configuración del sistema)



10. Seleccione **Cancel** (Cancelar) y pulse **Intro**. Se cierra la consola de configuración del sistema y aparece la indicación del shell de raíz.



11. Escriba **exit** (salir) y pulse **Intro**. Aparecerá la indicación de inicio de sesión.
12. Pulse **Ctrl + Alt** para salir del entorno de la consola.

Configuración de su appliance

Ahora está listo para configurar su appliance. Para configurar su appliance, consulte la **Guía de instalación y configuración de Stealthwatch** correspondiente a su versión de software. La serie x210 es compatible con las versiones de software 7.x de Stealthwatch.

Copyright Information