Cisco Stealthwatch

Guia de instalação de hardware da série x210

Table of Contents

Introdução

Descrição geral

Este guia explica como instalar os dispositivos de hardware Stealthwatch x210 Series. Descreve os componentes Stealthwatch e de que forma são integrados no sistema, incluindo a integração dos Sensores de fluxo. Este guia também descreve o procedimento de montagem e instalação do hardware Stealthwatch. O hardware da x210 Series inclui:

Aparelho	Número de peça
Coletor de fluxo Stealthwatch 4210	ST-FC4210-K9
Coletor de fluxo do Motor Stealthwatch 5210	ST-FC5210-E
Coletor de fluxo da Base de dados Stealthwatch 5210	ST-FC5210-D
Sensor de fluxo Stealthwatch 1210	ST-FS1210-K9
Sensor de fluxo Stealthwatch 3210	ST-FS3210-K9
Sensor de fluxo Stealthwatch 4210	ST-FS4210-K9
Consola de gestão Stealthwatch 2210	ST-SMC2210-K9
Encaminhador de UDP Stealthwatch 2210	ST-UDP2210-K9

Público-alvo

Este guia foi concebido para orientar a pessoa responsável pela instalação do hardware Stealthwatch. Parte-se do princípio de que o utilizador já tem conhecimentos gerais acerca da instalação de equipamento de rede (Sensor de fluxo, Coletor de fluxo, Encaminhador de UDP e a Consola de gestão Stealthwatch).

> Para obter informações acerca da configuração de dispositivos Stealthwatch, consulte o **Guia de configuração e instalação do Stealthwatch** aplicável à versão do seu software. A x210 Series é compatível com as versões 7.x do software Stealthwatch.

Como utilizar este guia

Para além desta introdução, este guia contém os seguintes capítulos:

Capítulo	Descrição
2 - **Considerações relativas à pré-configuração**	Os componentes Stealthwatch, o seu posicionamento e a configuração da firewall para as comunicações
3 - **Preparação da instalação**	Recomendações, avisos e orientações de segurança
4 - **Instalação**	Montagem e instalação de hardware Stealthwatch

Abreviaturas comuns

Neste guia, encontrará as seguintes abreviaturas:

Abreviatura	Descrição
DMZ	Zona desmilitarizada (uma rede de perímetro)
HTTPS	Hypertext Transfer Protocol (Seguro)
ISE	Identity Services Engine
NIC	Placa de Interface de rede
NTP	Network Time Protocol (Protocolo de sincronização da hora)
PCIe	Peripheral Component Interconnect Express
SNMP	Protocolo Simple Network Management
SPAN	Analisador de portas Switch
TAP	Porta de testes de acesso

Abreviatura	Descrição
UPS	Fonte de alimentação ininterrupta
VLAN	Rede local virtual

Preparação da instalação

Avisos relativos à instalação

Leia o documento Informações de segurança e conformidade regulamentar antes de instalar os dispositivos Stealthwatch x210 Series.

Tome nota dos seguintes avisos:

Declaração 1071—Definição de aviso

INSTRUÇÕES DE SEGURANÇA IMPORTANTES

Este símbolo de aviso significa perigo. Está numa situação que poderá causar lesão corporal. Antes de trabalhar em qualquer equipamento, tenha em atenção os perigos inerentes aos circuitos elétricos e familiarize-se com as práticas padrão para prevenção de acidentes. Utilize o número de declaração fornecido no final de cada aviso para localizar a respetiva tradução, nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

Declaração 1005—Disjuntor

Este produto confia na instalação elétrica do edifício no que respeita à proteção contra curto-circuito (sobretensão). Certifique-se de que a tensão nominal do dispositivo de proteção não é superior a: EUA: 120 V, 15 A (UE: 250 V, 16 A)

Declaração 1004—Instruções de instalação

Leia as instruções de instalação antes da utilização, instalação ou ligação do sistema à fonte de energia.

Declaração 12—Aviso de desconexão de fonte de alimentação

Antes de realizar trabalhos num chassi ou próximo de fontes de alimentação, desligue o cabo de alimentação nas unidades CA; desligue a alimentação no disjuntor nas unidades CC.

Declaração 43—Aviso de remoção de jóias

Antes de trabalhar em equipamento ligado à eletricidade, retire todas as jóias que estiver a usar (incluindo anéis, colares e relógios). Os objetos metálicos aquecem quando ligados à eletricidade e à terra e podem provocar queimaduras graves ou soldar o metal aos terminais.

Declaração 94—Aviso de pulseira

Durante este procedimento, utilize pulseiras de ligação à terra para evitar danos ESD no cartão. Não toque diretamente no barramento com a mão ou qualquer ferramenta metálica, pois pode apanhar um choque.

Declaração 1045—Proteção contra curto-circuito

Este produto necessita de proteção contra curto-circuito (sobretensão), a ser fornecida como parte da instalação do edifício. Instale apenas de acordo com os regulamentos de ligação nacionais e locais.

Declaração 1021—Circuito SELV

Para evitar choques elétricos, não ligue circuitos de tensão de segurança extra baixa (SELV) a circuitos de tensão da rede telefónica (TNV). As portas LAN contêm circuitos SELV e as portas WAN contêm circuitos TNV. Algumas portas LAN e WAN utilizam conectores RJ-45. Tenha cuidado ao ligar cabos.

Declaração 1024—Condutor de terra

Este equipamento precisa de ligação à terra. Nunca elimine o condutor de terra nem opere o equipamento sem o condutor de terra devidamente instalado. Contacte a autoridade de inspeção elétrica adequada ou um eletricista se tiver dúvidas sobre a existência de uma ligação à terra correta.

Declaração 1040—Eliminação do produto

A eliminação final deste produto deve ser realizada em conformidade com todas as leis e regulamentos nacionais.

Declaração 1074—Cumprimento dos códigos elétricos locais e nacionais

A instalação do equipamento deve respeitar os códigos elétricos locais e nacionais.

Declaração 19—Aviso relativo à alimentação TN

O dispositivo destina-se a funcionar com sistemas de alimentação TN.

Orientações de instalação

Tome nota dos seguintes avisos:

Declaração 1047—Prevenção de sobreaquecimento

Para evitar o sobreaquecimento do sistema não o opere em áreas cuja temperatura ambiente seja superior à máxima recomendada de: 5 a 40 °C.

Declaração 1019—Dispositivo de desconexão principal

A combinação ficha-tomada tem de estar sempre acessível, pois funciona como dispositivo de desconexão principal.

Declaração 1005—Disjuntor

Este produto confia na instalação elétrica do edifício no que respeita à proteção contra curto-circuito (sobretensão). Certifique-se de que a tensão nominal do dispositivo de proteção não é superior a: EUA: 120 V, 15 A (UE: 250 V, 16 A)

Declaração 1074—Cumprimento dos códigos elétricos locais e nacionais

A instalação do equipamento deve respeitar os códigos elétricos locais e nacionais.

Declaração 371 – Cabo de alimentação e adaptador AC

Utilize os cabos de ligação/cabos elétricos/adaptadores CA/baterias fornecidos ou designados para instalar o produto. A utilização de quaisquer outros cabos/adaptadores pode provocar avarias ou incêndio. A Lei relativa à

segurança dos dispositivos e materiais elétricos proíbe a utilização de cabos com certificação UL (com as letras "UL" ou "CSA" no cabo), não regulada pela lei ao mostrar "PSE" no cabo, em qualquer outro dispositivo elétrico além dos produtos concebidos pela CISCO.

Declaração 1073—Sem peças passíveis de assistência por parte do utilizador

Não existem peças passíveis de assistência por parte do utilizador. Não abrir.

Quando instalar um chassi, tenha em consideração as seguintes orientações:

- Certifique-se de que existe espaço suficiente em redor do chassi para poder efetuar manutenção e permitir um fluxo de ar adequado. No chassi, o fluxo de ar processa-se no sentido da parte frontal para a parte traseira.

  Para garantir que o fluxo de ar se processa corretamente, tem de montar o chassi no rack com os kits de calhas. Se colocar as unidades fisicamente empilhadas umas sobre as outras sem os kits de calhas, vai bloquear os orifícios de ventilação existentes na parte superior do chassi, o que pode provocar sobreaquecimento, um aumento da velocidade das ventoinhas e um maior consumo de energia. Quando instalar o chassi no rack, recomenda-se que o monte com os kits de calhas, uma vez que estes garantem o espaçamento mínimo necessário entre o chassi e o rack. Se montar o chassi com os kits de calhas, não tem de acrescentar qualquer espaçamento adicional entre chassi e o rack.

- Certifique-se de que o ar condicionado tem capacidade para manter o chassi a uma temperatura de 5 a 35 °C.
- Certifique-se de que o armário ou o rack estão em conformidade com os requisitos de rack.
- Certifique-se de que a alimentação no local está em conformidade com os requisitos de alimentação indicados na folha de especificações do seu dispositivo. Se disponível, pode utilizar uma UPS como proteção contra falhas de alimentação.

  Evite os tipos de UPS que utilizam tecnologia ferrorressonante. Estes tipos de UPS podem tornar-se instáveis com estes sistemas, que podem ter flutuações de consumo de corrente substanciais devido a padrões de tráfego de dados irregulares.

Recomendações de segurança

As informações a seguir ajudam a garantir a sua segurança e a proteger o chassi. Estas informações podem não abranger todas as situações potencialmente perigosas no seu ambiente de trabalho, por isso, esteja atento e avalie sempre bem cada situação.

Observe estas diretrizes de segurança:

- Mantenha a área desimpedida e sem pó antes, durante e após a instalação.
- Mantenha as ferramentas afastadas das áreas de passagem onde o utilizador ou outras pessoas possam tropeçar nas mesmas.
- Não use vestuário largo nem jóias, como brincos, pulseiras ou colares que possam ficar presos no chassi.
- Use óculos de segurança se trabalhar em condições que possam ser perigosas para os olhos.
- Não realize qualquer ação que represente um perigo para as pessoas ou que afete a segurança do equipamento.
- Nunca tente elevar um objeto demasiado pesado para uma só pessoa.

Manter a segurança elétrica

> ⚠ Antes de realizar trabalhos num chassi, certifique-se de que o cabo de alimentação foi desligado.

Respeite estas orientações ao operar equipamento alimentado a eletricidade:

- Não trabalhe sozinho quando existam condições perigosas no seu espaço de trabalho.
- Nunca presuma que a eletricidade está desligada; verifique sempre.
- Observe bem a sua área de trabalho para detetar eventuais perigos, como pisos húmidos, cabos de extensões elétricas sem ligação à terra, cabos elétricos desgastados e ausência de ligações à terra de segurança.
- Se ocorrer um acidente elétrico:
  - Tenha cuidado para não se magoar.
  - Desligue a alimentação do sistema.
  - Se possível, peça a outra pessoa para chamar assistência médica. Caso contrário, avalie o estado da vítima e, em seguida, solicite socorro.
  - Determine se a pessoa precisa de respiração cardiopulmonar ou de compressões torácicas e atue em conformidade.

- Utilize o chassi de acordo com as especificações elétricas assinaladas e as instruções de utilização do produto.

Prevenção de danos resultantes de descarga eletrostática (ESD)

As descargas eletrostáticas (ESD) ocorrem quando os componentes eletrónicos são manuseados incorretamente e podem danificar o equipamento, bem como afetar os circuitos elétricos, o que pode provocar avarias intermitentes ou a avaria total do seu equipamento.

Siga sempre os procedimentos de prevenção de ESD quando remover e substituir componentes. Assegure-se de que o chassi está eletricamente ligado à terra. Use uma pulseira anti-ESD e certifique-se de que esta está sempre em contacto com a pele. Prenda a presilha de ligação à terra numa superfície não pintada da frame do chassi para encaminhar tensões de ESD de forma segura para a terra. Para prevenir devidamente danos e choques decorrentes de ESD, a pulseira e o cabo têm de funcionar eficazmente. Caso não disponha de uma pulseira, proteja-se tocando numa parte metálica do chassi.

Por motivos de segurança, verifique periodicamente o valor de resistência da pulseira antiestática, que deve situar-se entre um e 10 megohms.

Ambiente do local

Para evitar avarias no equipamento e reduzir a possibilidade de encerramentos provocados pelas condições do ambiente, planeie cuidadosamente a configuração do local e a localização do equipamento. Se verificar que estão a ocorrer encerramentos frequentes ou se existirem taxas de erro invulgarmente elevadas no seu equipamento, pode ser útil isolar a causa dessas falhas e evitar problemas futuros.

Considerações sobre a fonte de alimentação

Quando instalar o chassi, considere o seguinte:

- Assegure a existência de alimentação no local antes de instalar o chassi para garantir que está livre de picos e ruído. Se necessário, instale um condicionador de potência, para assegurar as tensões corretas e níveis de potência corretos na tensão de entrada do dispositivo.
- Instale uma ligação à terra correta para evitar danos provocados por relâmpagos e picos de corrente no local.

- O chassi não tem um intervalo de operação selecionável pelo utilizador. Consulte a identificação no chassi relativa ao requisito de potência de entrada correta do dispositivo.
- Estão disponíveis vários tipos de cabos de alimentação CA para o dispositivo; certifique-se de que possui o tipo adequado ao seu local.
- Se estiver a utilizar fontes de alimentação redundantes duplas (1+1), recomendamos que utilize circuitos elétricos independentes para cada fonte de alimentação.
- Instale uma fonte de alimentação ininterrupta no seu local, se possível.

Considerações relativas à configuração do rack

Considere o seguinte quando planear uma configuração de rack:

- Assegure-se de que a frame do bastidor não bloqueia as portas de admissão e de exaustão se estiver a montar um chassi num bastidor aberto.
- Assegure que os bastidores fechados possuem uma ventilação adequada. Certifique-se de que o bastidor não está demasiado congestionado, já que cada chassi produz calor. Os bastidores fechados devem ter laterais em persiana e uma ventoinha para fornecer ar de ventilação.
- Num bastidor fechado com uma ventoinha de ventilação na parte superior, o calor produzido pelo equipamento próximo da parte inferior do bastidor pode ser puxado para cima e para dentro das portas de admissão do equipamento que se encontra por cima, no bastidor. Assegure uma ventilação adequada no equipamento na parte inferior do bastidor.
- A utilização de defletores pode ajudar a isolar o ar de exaustão do ar de admissão, ajudando também a captar o ar de ventilação através do chassi. O melhor posicionamento dos defletores depende dos padrões de fluxo de ar do bastidor. Experimente diferentes disposições para posicionar os defletores da forma mais eficaz.

Considerações relativas à pré-configuração

Esta secção aborda os aspetos a considerar antes de instalar e configurar os seus dispositivos Stealthwatch. Explica onde colocar os dispositivos Stealthwatch e como os integrar na sua rede. Inclui:

- **Início de sessão com a palavra-passe predefinida CIMC**
- **Acerca dos dispositivos Stealthwatch**
- **Posicionamento dos dispositivos**
- **Portas de comunicação**
- **Integração do Sensor de fluxo na sua rede**

Início de sessão com a palavra-passe predefinida CIMC

O Cisco Integrated Management Controller (CIMC) permite o acesso à configuração do servidor e a uma consola do servidor virtual, para além de monitorizar o estado do hardware. Utilize a seguinte palavra-passe predefinida para iniciar sessão no CIMC:

`password`.

Depois de iniciar sessão, altere a palavra-passe predefinida para garantir a segurança da sua rede.

Acerca dos dispositivos Stealthwatch

A gama Stealthwatch inclui vários dispositivos de hardware que recolhem, analisam e apresentam informações acerca da sua rede e permitem melhorar o desempenho e a segurança da rede. Esta secção descreve todos os dispositivos Stealthwatch x210 Series.

> Para obter mais informações, consulte as folhas de especificações de cada dispositivo Stealthwatch x210 Series.

Consola de gestão Stealthwatch 2210

A Consola de gestão Stealthwatch gere, coordena, configura e organiza todos os diferentes componentes do sistema. O software Stealthwatch permite aceder à IU Web da consola a partir de qualquer computador com um browser Web. Pode aceder facilmente a informações de segurança e de rede, em tempo real, relativas a segmentos críticos de

todas a sua empresa. Com uma plataforma independente baseada em Java, a Consola de gestão Stealthwatch permite:

- Efetuar a gestão, configuração e criação de relatórios centralizadas de até 25 coletores de fluxo Stealthwatch
- Obter gráficos de imagem para visualizar o tráfego
- Efetuar uma análise detalhada para resolver problemas
- Obter relatórios consolidados e personalizáveis
- Efetuar a análise de tendências
- Monitorização do desempenho
- Obter notificações imediatas se ocorrerem falhas de segurança

Coletores de fluxo Stealthwatch 4210 e 5210

O Coletor de fluxo Stealthwatch recolhe dados NetFlow, cFlow, J-Flow, Packeteer 2, NetStream e IPFIX para proporcionar uma proteção da rede baseada em comportamentos.

O Coletor de fluxo agrega dados comportamentais da rede de alta velocidade a partir de várias redes ou de segmentos da rede, para proporcionar uma proteção abrangente e melhorar o desempenho em várias redes dispersas geograficamente.

> À medida que o Coletor de fluxo recebe os dados, identifica ataques conhecidos ou desconhecidos, má utilização a nível interno e dispositivos de rede incorretamente configurados, independentemente da encriptação ou da fragmentação de pacotes. Assim que o Stealthwatch identifica o comportamento, o sistema pode tomar quaisquer medidas que tenha configurado, em relação a qualquer tipo de comportamento.

Sensores de fluxo Stealthwatch 1210, 3210 e 4210

O Sensor de fluxo Stealthwatch é um dispositivo de rede com um funcionamento semelhante a um dispositivo de captura de pacotes tradicional ou a um IDS, pelo facto de se poder ligar a analisador de portas do switch (SPAN), a uma porta de espelhamento ou a uma porta Ethernet de testes de acesso (TAP). O Sensor de fluxo aumenta a visibilidade nas seguintes áreas da rede:

- Onde não existe NetFlow.
- Onde existe NetFlow, mas pretende obter uma maior visibilidade das métricas de desempenho e dos dados de pacote.

Ao direcionar o Sensor de fluxo para qualquer coletor de fluxo compatível com NetFlow v9, pode obter estatísticas de tráfego detalhadas valiosas a partir do NetFlow. Quando combinado com o Coletor de fluxo Stealthwatch, o Sensor de fluxo também fornece informações detalhadas acerca das métricas de desempenho e dos indicadores comportamentais. Estes indicadores de desempenho de fluxo permitem obter informações acerca de qualquer latência de ida e volta que possa ter sido introduzida pela rede ou pela aplicação do lado do servidor.

Como o Sensor de fluxo oferece visibilidade ao nível dos pacotes, pode calcular o tempo de ida e volta (RTT), o tempo de resposta do servidor (SRT) e a perda de pacotes em sessões de TCP. Inclui todos estes campos adicionais nos registos NetFlow que envia para o Coletor de fluxo.

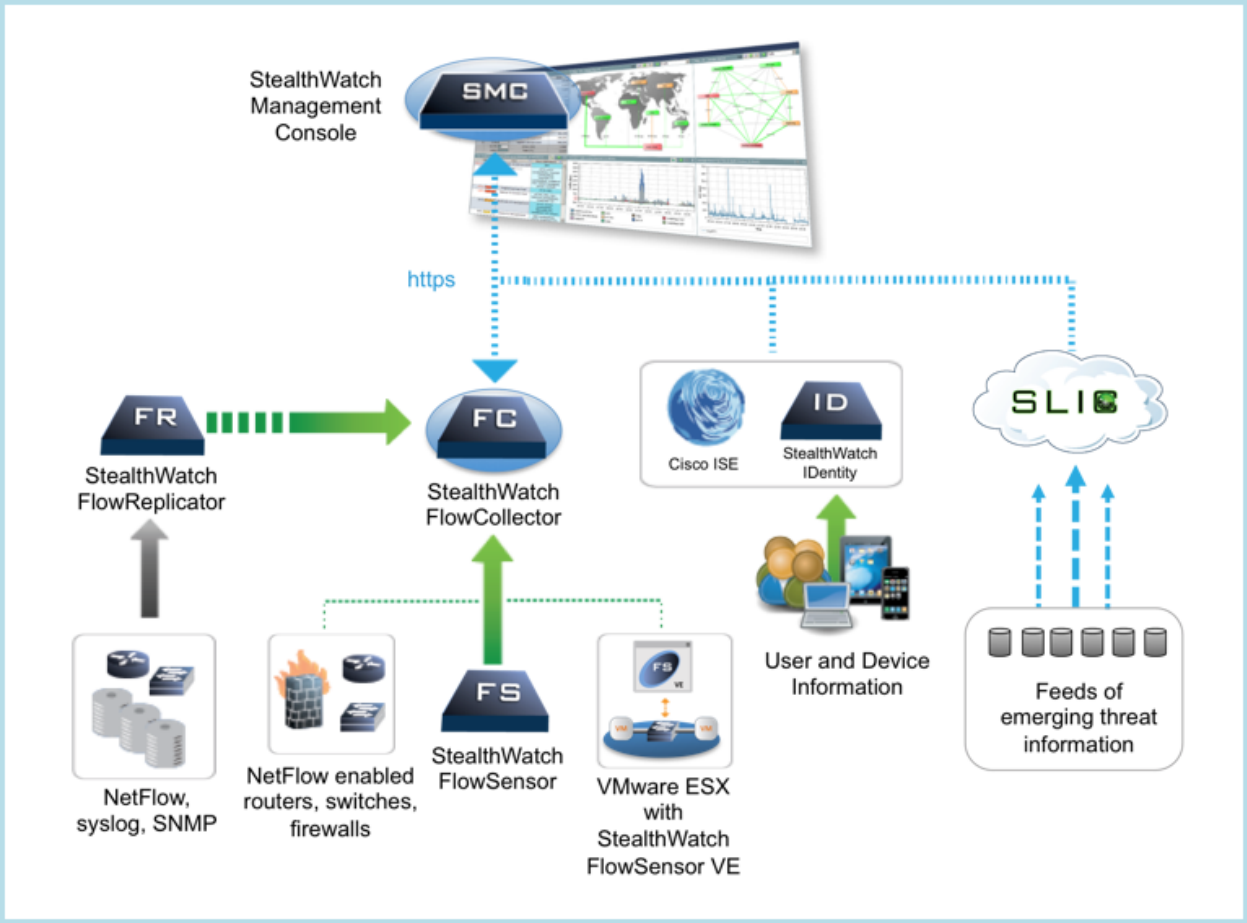
Encaminhador de UDP Stealthwatch 2210

O Encaminhador de UDP Stealthwatch é um replicador de pacotes UDP de alta velocidade e alto desempenho. O Encaminhador de UDP é muito útil para redistribuir traps NetFlow, sFlow, syslog ou Simple Network Management Protocol (SNMP) por vários coletores. Pode receber dados provenientes de qualquer aplicação UDP sem ligação e, posteriormente, retransmiti-los para vários destinos, para além de poder duplicar os dados, se tal for necessário.

Para utilizar a configuração de elevada disponibilidade (HA) do Encaminhador de UDP (ativação pós-falha), tem de ligar dois dispositivos de Encaminhador de UDP através de cabos crossover. Para obter instruções específicas, consulte **Ligação do dispositivo à rede**.

Posicionamento dos dispositivos

Conforme apresentado na figura abaixo, pode implementar estrategicamente dispositivos Stealthwatch para obter uma cobertura ótima de segmentos chave da rede em toda a rede, seja uma rede interna, uma rede no perímetro ou no DMZ.



Posicionamento da Consola de gestão Stealthwatch

Instale a Consola de gestão Stealthwatch como dispositivo de gestão numa localização da sua rede que seja acessível a todos os dispositivos que enviam dados para a mesma.

Se tiver o par de ativação pós-falha de Consolas de gestão Stealthwatch, recomenda-se que instale a consola primária e a consola secundária em localizações físicas separadas. Esta estratégia otimiza qualquer esforço de recuperação de desastres, caso seja necessário.

Posicionamento do Coletor de fluxo Stealthwatch

Enquanto dispositivo de recolha e monitorização, o Coletor de fluxo Stealthwatch deve ser instalado num local da sua rede que seja acessível aos dispositivos NetFlow ou sFlow que enviam dados para um Coletor de fluxo, bem como quaisquer dispositivos que planeie utilizar para aceder à interface de gestão.

Quando coloca um Coletor de fluxo fora de uma firewall, recomenda-se que desative a definição **Accept traffic from any exporter** (Aceitar tráfego proveniente de qualquer exportador).

Posicionamento do Sensor de fluxo Stealthwatch

Enquanto dispositivo de monitorização passiva, o Sensor de fluxo Stealthwatch pode ser colocado em vários pontos da sua rede para observar e registar a atividade IP, o que permite proteger a integridade da rede e detetar falhas de segurança. O Sensor de fluxo possui sistemas de gestão baseados na Web integrados que permitem efetuar a gestão e administração centralizada ou remota.

O dispositivo Sensor de fluxo é mais eficaz se for colocado em segmentos críticos da sua rede corporativa, conforme indicado a seguir:

- Dentro da firewall, para monitorizar o tráfego e determinar se ocorreu uma falha da firewall
- Fora da firewall, para monitorizar o fluxo do tráfego e analisar quem está a ameaçar a firewall
- Em segmentos sensíveis da sua rede, para oferecer proteção contra funcionários descontentes ou piratas informáticos com acesso de raiz
- Em localizações remotas do escritório que são extensões da rede vulneráveis
- Na sua rede empresarial para a gestão de utilização de protocolos (por exemplo, na sub-rede de serviços de transações para determinar se um pirata informático está a utilizar Telnet ou FTP e a comprometer os dados financeiros do seu cliente)

Posicionamento do Encaminhador de UDP Stealthwatch

Relativamente ao posicionamento do Encaminhador de UDP Stealthwatch, apenas se exige que tenha um caminho de comunicação desimpedido para comunicar com os seus outros dispositivos Stealthwatch.

Configuração da Firewall para as comunicações

Para os dispositivos comunicarem corretamente, deve configurar a rede de forma que as firewalls ou as listas de controlo de acesso não bloqueiem as ligações necessárias. Utilize o diagrama e as tabelas apresentados nesta secção para configurar a sua rede de forma que os dispositivos possam comunicar através da rede.

Contacte o administrador da sua rede para garantir que as seguintes portas estão abertas e têm acesso sem restrições:

- 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

Portas de comunicação

A tabela seguinte indica como são utilizadas as portas no Stealthwatch:

De (Cliente)	Para (Servidor)	Porta	Protocolo
PC do Utilizador Admin	Todos os dispositivos	TCP/443	HTTPS
Todos os dispositivos	Origem da hora da rede	UDP/123	NTP
Active Directory	Consola de gestão Stealth-watch	TCP/389, UDP/389	LDAP
AnyConnect	Ponto final Concentrador	UDP/2055	NetFlow
Cisco ISE	Consola de gestão Stealth-watch	TCP/443	HTTPS
Cisco ISE	Consola de gestão Stealth-watch	TCP/5222	XMPP
Concentrador do ponto final	Coletor de fluxo	UDP/2055	NetFlow
Origens de registo externas	Consola de gestão Stealth-watch	UDP/514	SYSLOG
Coletor de fluxo	Consola de gestão Stealth-watch	TCP/443	HTTPS
SLIC	Consola de gestão Stealth-watch	TCP/443 ou ligação com proxy	HTTPS
Encaminhador de UDP	Coletor de fluxo - sFlow	UDP/6343	sFlow
Encaminhador de UDP	Coletor de fluxo - NetFlow	UDP/2055*	NetFlow
Encaminhador de UDP	Sistemas de gestão de eventos de terceiros	UDP/514	syslog

De (Cliente)	Para (Servidor)	Porta	Protocolo
Sensor de fluxo	Consola de gestão Stealth-watch	TCP/443	HTTPS
Sensor de fluxo	Coletor de fluxo - NetFlow	UDP/2055	NetFlow
Identidade	Consola de gestão Stealth-watch	TCP/2393	SSL
Exportadores NetFlow	Coletor de fluxo - NetFlow	UDP/2055*	NetFlow
Exportadores sFlow	Coletor de fluxo - sFlow	UDP/6343*	sFlow
Consola de gestão Stealthwatch	Cisco ISE	TCP/443	HTTPS
Consola de gestão Stealthwatch	DNS	UDP/53	DNS
Consola de gestão Stealthwatch	Coletor de fluxo	TCP/443	HTTPS
Consola de gestão Stealthwatch	Sensor de fluxo	TCP/443	HTTPS
Consola de gestão Stealthwatch	Identidade	TCP/2393	SSL
Consola de gestão Stealthwatch	Exportadores de fluxo	UDP/161	SNMP
Consola de gestão Stealthwatch	Concentrador do ponto final	UDP.2055	HTTPS
PC do utilizador	Consola de gestão Stealth-watch	TCP/443	HTTPS

*Esta é a porta predefinida, mas pode configurar qualquer porta UDP no exportador.

A tabela seguinte indica as configurações opcionais determinadas pelas necessidades da sua rede:

De (Cliente)	Para (Servidor)	Porta	Protocolo
Todos os dispositivos	PC do utilizador	TCP/22	SSH
Consola de gestão Stealthwatch	Gestão de eventos de terceiros	UDP/162	SNMP-trap
Consola de gestão Stealthwatch	Gestão de eventos de terceiros	UDP/514	syslog
Consola de gestão Stealthwatch	Gateway de e-mail	TCP/25	SMTP
Consola de gestão Stealthwatch	SLIC	TCP/443	SSL
PC do utilizador	Todos os dispositivos	TCP/22	SSH

O diagrama seguinte indica as várias ligações utilizadas pelo Stealthwatch. As portas assinaladas como opcionais são as que pode utilizar, de acordo com as necessidades da sua própria rede.

Integração do Sensor de fluxo na sua rede

O Sensor de fluxo Stealthwatch é versátil e pode ser integrado numa grande variedade de topologias, tecnologias e componentes de rede. Embora não seja possível abordar todas as configurações de rede neste documento, os exemplos podem ajudar a determinar qual é a melhor configuração para as suas necessidades.

Antes de instalar um Sensor de fluxo, tem de tomar várias decisões acerca da sua rede e sobre como a pretender monitorizar. Certifique-se de que analisa a topologia da sua rede e as suas necessidades de monitorização específicas. Recomenda-se que ligue um Sensor de fluxo para que este receba as transmissões de rede enviadas para e recebidas pela rede monitorizada e, se pretender, para que receba também transmissões de rede interna.

As secções seguintes explicam como integrar um dispositivo Sensor de fluxo Stealthwatch na sua rede com os seguintes dispositivos de rede Ethernet:

- **TAPs**
- **Portas SPAN**

TAPs

Quando uma Porta de testes de acesso (TAP) está em linha com uma ligação de rede, repete a ligação numa porta ou em portas separadas. Por exemplo, uma TAP Ethernet colocada em linha com um cabo Ethernet vai repetir todas as direções de transmissão em portas separadas. Consequentemente, a TAP é a forma mais fiável de utilizar o Sensor de fluxo. O tipo de TAP que utiliza depende da sua rede.

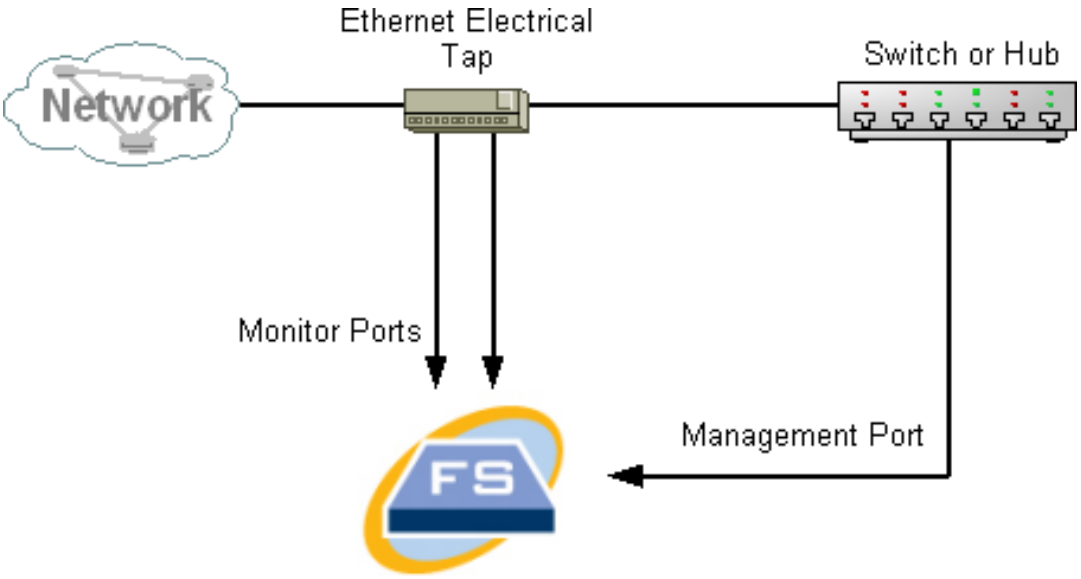
Esta secção explica as seguintes formas de utilizar TAPs:

- **Utilizar TAPs elétricas**
- **Utilizar TAPs óticas**
- **Utilizar TAPs fora da sua firewall**
- **Colocar o Flow Sensor dentro da Firewall**

Numa rede que utiliza TAPs, o Sensor de fluxo apenas pode captar os dados de monitorização do desempenho se estiver ligado a uma TAP de agregação que esteja a captar o tráfego de entrada e também o de saída. Se o Sensor de fluxo estiver ligado a uma TAP unidirecional que esteja a captar apenas uma direção do tráfego em cada porta, o Sensor de fluxo não vai captar os dados de monitorização do desempenho.

Utilizar TAPs elétricas

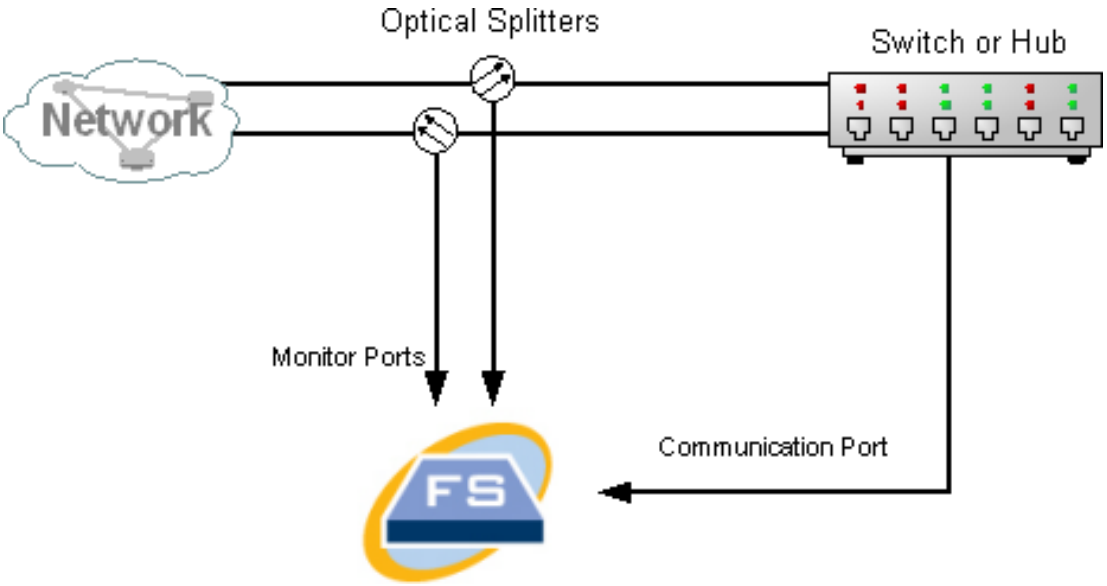
No exemplo abaixo, o Sensor de fluxo está ligado a uma TAP de Ethernet elétrica. Para tal, ligue as duas portas TAP às portas Monitor 1 e 2 do Sensor de fluxo.



Utilizar TAPs óticas

Em sistemas de fibra ótica, utilize dois divisores. Coloque um divisor de cabo de fibra ótica em linha com cada direção de transmissão para repetir o sinal ótico para uma direção de transmissão.

No exemplo abaixo, o Sensor de fluxo está ligado a uma rede baseada em fibra ótica. Para tal, ligue as saídas dos divisores às portas Monitor 1 e 2 do Sensor de fluxo.



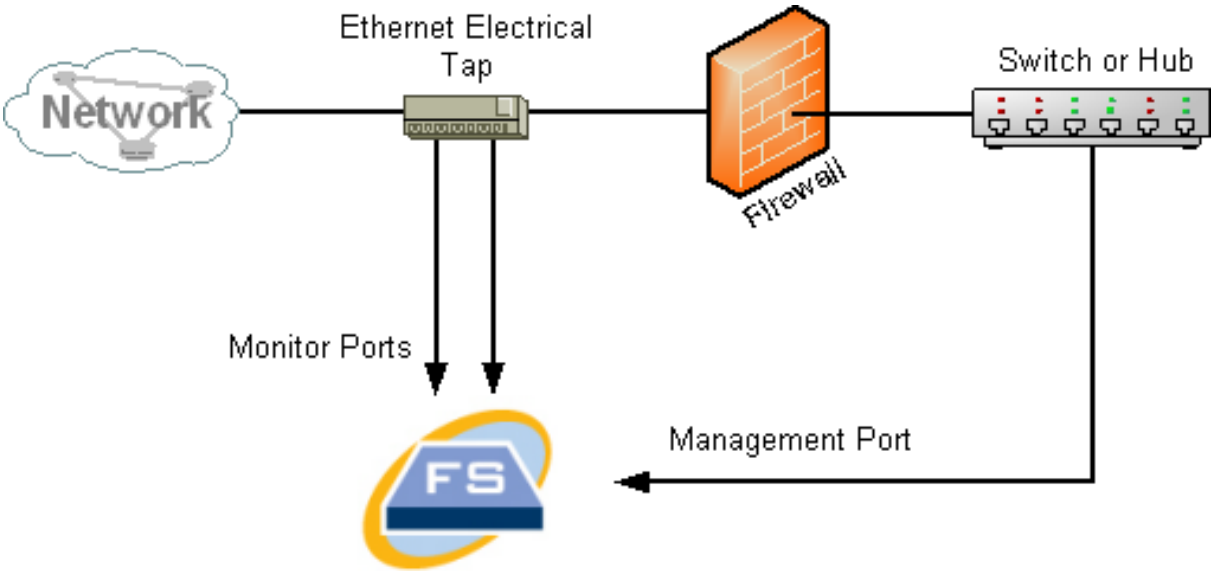
Se existir uma ligação de fibra ótica entre as redes monitorizadas, o Sensor de fluxo é ligado a dois divisores óticos. A porta de gestão é ligada ao switch da rede monitorizada ou a outro switch ou hub.

Utilizar TAPs fora da sua firewall

Para o Sensor de fluxo monitorizar o tráfego entre a sua firewall e outras redes, ligue a porta de gestão Stealthwatch a um switch ou a uma porta fora da firewall.

Recomenda-se vivamente que utilize uma TAP para estabelecer esta ligação, de forma a que a avaria do dispositivo não desative completamente a sua rede.

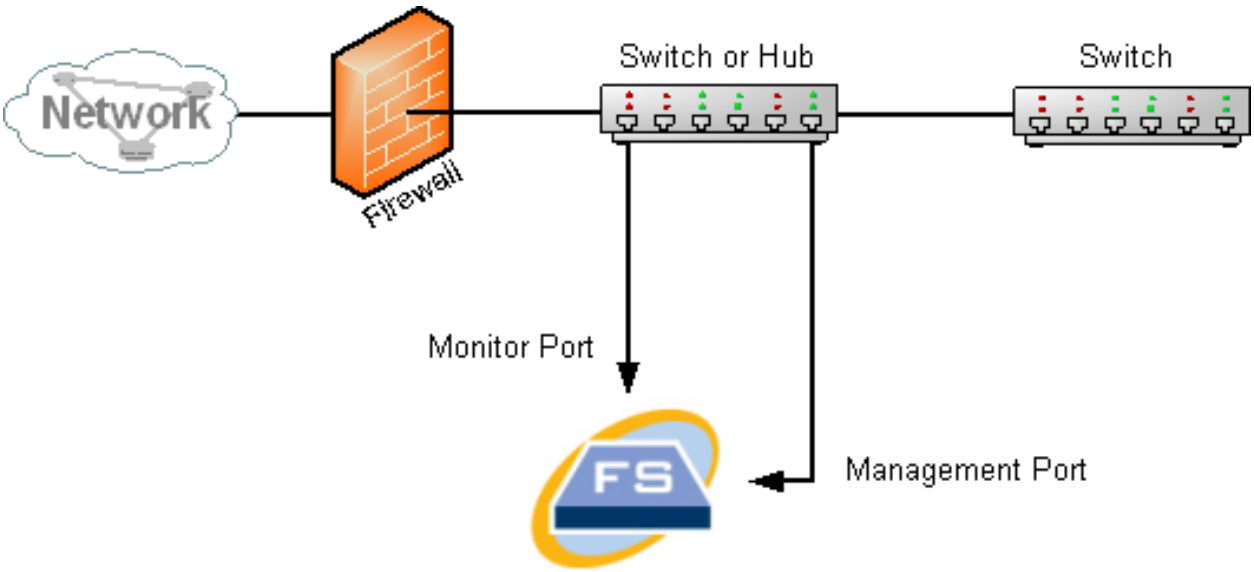
O exemplo abaixo mostra a utilização de uma TAP de Ethernet elétrica. A porta de gestão tem de ser ligada ao switch ou ao hub da rede monitorizada. Esta configuração é semelhante à configuração que monitoriza o tráfego enviado e recebido pela sua rede.



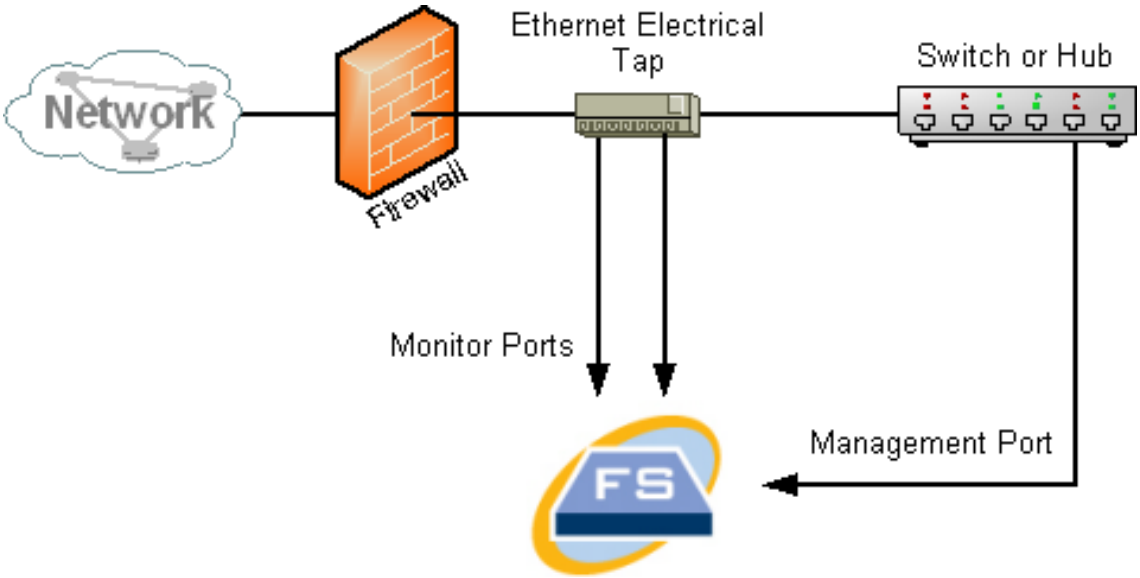
Se a sua firewall estiver a executar a tradução de endereços de rede (NAT), apenas pode observar os endereços que estão na firewall.

Colocar o Flow Sensor dentro da Firewall

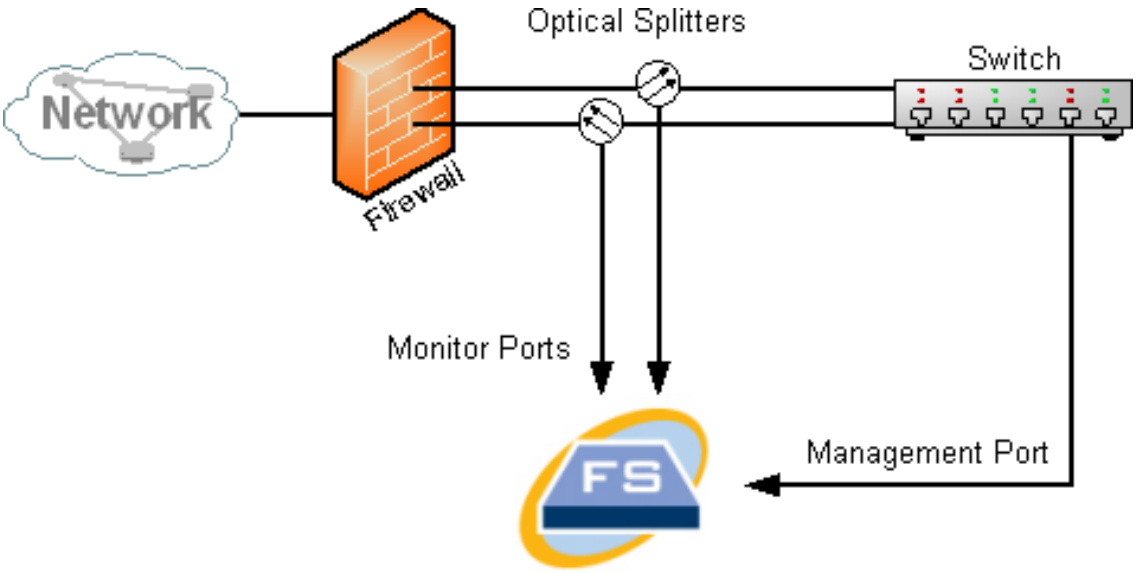
Para monitorizar o tráfego entre redes internas e uma firewall, o Sensor de fluxo tem de poder aceder a todo o tráfego entre a firewall e as redes internas. Para tal, configure uma porta de espelhamento que replique a ligação à firewall no switch principal. Certifique-se de que a porta Monitor 1 do Sensor de fluxo está ligada à porta de espelhamento, conforme apresentado na ilustração a seguir:



Para monitorizar o tráfego dentro da sua firewall com uma TAP, insira a TAP ou o divisor ótico entre a firewall e o switch ou hub principal. A configuração da TAP é apresentada abaixo.



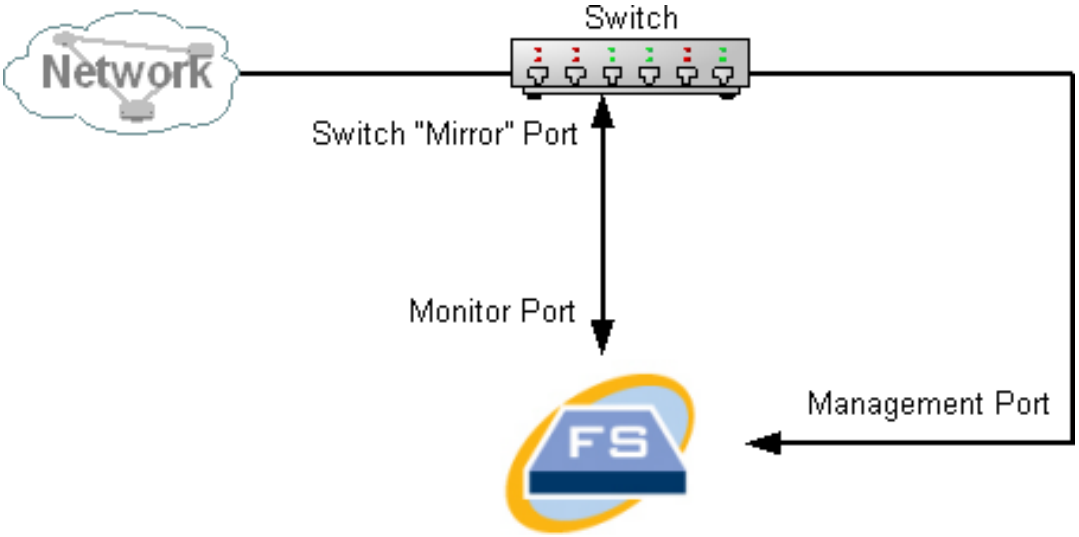
A configuração do divisor ótico é apresentada abaixo.



Portas SPAN

Também pode ligar o Sensor de fluxo a um switch. No entanto, como um switch não repete todo o tráfego em cada porta, o Sensor de fluxo não funcionará corretamente, a menos que o switch seja capaz de repetir os pacotes recebidos e enviados através de uma ou mais portas switch. Este tipo de porta de switch é frequentemente designado de porta de espelhamento ou analisador de portas switch (SPAN).

A ilustração a seguir mostra como pode obter esta configuração ao ligar a sua rede ao Sensor de fluxo Stealthwatch através da porta de gestão.



Nesta configuração, também tem de configurar uma porta do switch (também designada de porta de espelhamento), para que esta repita todo o tráfego enviado e recebido pelos

anfitriões de interesse para a porta de espelhamento. A porta Monitor 1 do Sensor de fluxo tem de ser ligada a esta porta de espelhamento. Tal permite que o Sensor de fluxo monitorize o tráfego enviado e recebido pela rede de interesse e para outras redes. Nesta instância, uma rede pode ser formada por alguns ou por todos os anfitriões ligados ao switch.

Uma forma comum de configurar redes num switch consiste em criar zonas de redes locais virtuais (VLANs), que são ligações lógicas, em vez de físicas, de anfitriões. Se a porta de espelhamento estiver configurada para espelhar todas as portas de uma VLAN ou de um switch, o Sensor de fluxo pode monitorizar todos o tráfego enviado, recebido e interno da rede de interesse, bem como de outras redes.

Em todos os casos, recomenda-se que consulte a documentação do fabricante do seu switch para determinar como configurar a porta de espelhamento do switch e qual será o tráfego que será repetido para porta de espelhamento.

Instalação

Esta secção aborda a instalação dos dispositivos no seu ambiente. Inclui:

- **Montagem do dispositivo**
- **Ligação do dispositivo à rede**
- **Ligação do dispositivo**
- **Alteração de informações predefinidas**

Montagem do dispositivo

Pode montar os dispositivos Stealthwatch diretamente num rack ou armário padrão de 19", em qualquer outro armário adequado ou sobre uma superfície plana. Quando montar um dispositivo num rack ou num armário, siga as instruções incluídas nos kits de calhas de montagem. Quando determinar o local onde o equipamento ficará montado, certifique-se de que deixa uma folga nos painéis frontal e traseiro para que:

- Os indicadores do painel frontal sejam fáceis de ler
- O espaço de acesso às portas do painel traseiro seja suficiente para não limitar a cablagem
- A tomada de alimentação do painel traseiro fique perto de uma fonte de alimentação AC condicionada
- O fluxo de ar em torno do dispositivo e no interior das condutas não apresente restrições.

Hardware incluído com o dispositivo

Os dispositivos Stealthwatch incluem o seguinte hardware:

- Cabo de alimentação CA
- Chaves de acesso (para a superfície frontal da placa)
- Kit de calhas para montagem em rack ou abas de montagem para dispositivos mais pequenos
- Para o Coletor de fluxo 5210, um cabo de SFP de 10 GB

Hardware adicional necessário

Tem de fornecer o seguinte hardware adicional necessário:

- Parafuso de montagem para um rack padrão de 19"
- Uma fonte de alimentação ininterrupta (UPS) para cada dispositivo que instalar
- Para efetuar a configuração local (opcional), recorra a um dos seguintes métodos:
  - Computador portátil com um cabo de vídeo e um cabo USB (para o teclado)
  - Monitor de vídeo com um cabo de vídeo e um teclado com um cabo USB

Ligação do dispositivo à rede

Utilize o mesmo procedimento para ligar todos os dispositivos à rede. Em termos de ligação, a única diferença consiste no tipo de dispositivo que tem.

Para obter informações detalhadas relativas às especificações, consulte as Folhas de especificações Stealthwatch.

> Todo o hardware Cisco x210 utiliza a mesma plataforma UCS, a UCSC-C220-M5SX, exceto o Coletor de fluxo 5210 DB, que utiliza a UCSC-C240-M5SX. As diferenças entre dispositivos estão nas placas NIC, no processador, na memória, no armazenamento e no RAID.

> O Coletor de fluxo 5210 é composto por dois servidores ligados (motor e base de dados) e funciona como um único dispositivo. Devido a isso, a instalação é ligeiramente diferente da de outros dispositivos. Primeiro, ligue os servidores entre si através de um cabo 10G SFP+ DA Cross Connect. Em seguida, ligue-os à sua rede.

Para ligar o dispositivo à rede:

1. Ligue um cabo Ethernet à porta de gestão, situada na parte traseira do dispositivo.
2. Ligue, pelo menos, uma porta de monitorização para os Sensores de fluxo e para os Encaminhadores de UDP.

   No caso do Encaminhador de UDP HA, ligue os Encaminhadores de UDP através de cabos crossover. Ligue a porta eth2 de um Encaminhador de UDP à porta eth2 do segundo Encaminhador de UDP. Da mesma forma, ligue a porta eth3 de cada Encaminhador de UDP com um segundo cabo crossover. O cabo pode ser de fibra ótica ou em cobre.

   Certifique-se de que toma nota da etiqueta Ethernet (eth2, eth3, etc.) de cada porta. Estas etiquetas correspondem às interfaces de rede (eth2, eth3, etc.) que

são apresentadas e podem ser configuradas na página Inicial da interface de administrador do dispositivo.

3. Ligue a outra extremidade dos cabos Ethernet ao switch da sua rede.
4. Ligue os cabos de alimentação à fonte de alimentação. Alguns dispositivos têm duas ligações de alimentação: Power Supply 1 e Power Supply 2.

Ligação do dispositivo

Esta secção descreve como ligar o dispositivo de forma a alterar as palavras-passe de utilizador predefinidas.

Pode ligar o dispositivo através uma das seguintes formas:

- com um teclado e um monitor
- com um computador portátil (e um emulador de terminal)

No caso de dispositivos novos, o SSH está desativado. Tem de iniciar sessão na interface da Web de administrador do dispositivo para o ativar.

Ligação com um teclado e um monitor

Para configurar localmente o endereço IP, siga os passos abaixo:

1. Ligue o cabo de alimentação ao dispositivo.
2. Prima o botão Power para ligar o dispositivo. Aguarde até concluir totalmente o arranque. Não interrompa o processo de arranque.

> Pode ter de remover o painel frontal para ligar a alimentação.
>
> Enquanto o sistema não arranca, as ventoinhas da fonte de alimentação de alguns modelos ligam-se. Verifique se o indicador LED no painel frontal está ativo.
>
> Certifique-se de que liga o dispositivo a uma fonte de alimentação ininterrupta (UPS). A fonte de alimentação tem de estar ligada à energia, caso contrário, o sistema apresenta um erro.

3. Ligar o teclado:
   - Se tiver um teclado padrão, ligue-o ao conetor de teclado padrão.
   - Se tiver um teclado USB, ligue-o a um conetor USB.
4. Ligue o cabo de vídeo ao conetor de vídeo. É apresentada a linha de comandos de início de sessão.
5. Continue para a secção **Alteração de informações predefinidas**.

Ligação com um computador portátil

Também pode ligar o dispositivo a um computador portátil que tenha um emulador de terminal.

Para ligar um dispositivo com um computador portátil:

1. Ligue o computador portátil ao dispositivo através de um dos seguintes métodos:
   - Ligue um cabo RS232 do conetor de porta de série (DB9) do seu portátil à porta Console do dispositivo.
   - Ligue um cabo crossover da porta Ethernet do portátil à porta Management do dispositivo.
2. Ligue o cabo de alimentação ao dispositivo.
3. Prima o botão Power para ligar o dispositivo. Aguarde até concluir totalmente o arranque. Não interrompa o processo de arranque.

   > Pode ter de remover o painel frontal para ligar a alimentação.
   >
   > Enquanto o sistema não arranca, as ventoinhas da fonte de alimentação de alguns modelos ligam-se. Verifique se o indicador LED no painel frontal está ativo. Certifique-se de que liga o dispositivo a uma fonte de alimentação ininterrupta (UPS). A fonte de alimentação tem de estar ligada à energia, caso contrário, o sistema apresenta um erro.

4. No computador portátil, estabeleça ligação ao dispositivo.

   Pode utilizar qualquer emulador de terminal que tiver disponível para comunicar com o dispositivo.

5. Aplique as seguintes definições:
   - BPS: 115200
   - Bits de dados: 8
   - Bit de paragem: 1
   - Paridade: Nenhuma
   - Controlo do fluxo: Nenhum

   São apresentados o ecrã e a linha de comandos de início de sessão.

6. Continue para a secção seguinte, **Alteração de informações predefinidas**.

Alteração de informações predefinidas

Depois de estabelecer ligação ao dispositivo, configure os endereços IP e altere as palavras-passe de utilizador.

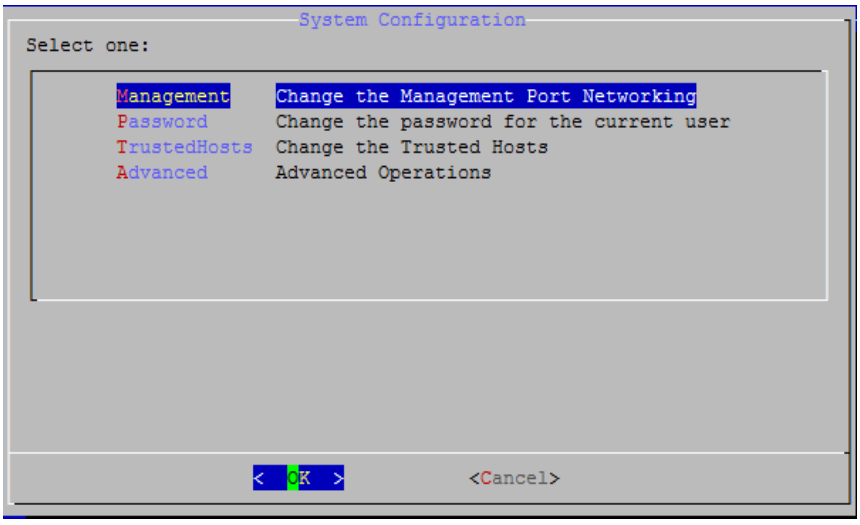
Alteração dos endereços IP predefinidos

Os dispositivos já possuem endereços IP predefinidos, mas deve configurá-los para a sua rede.

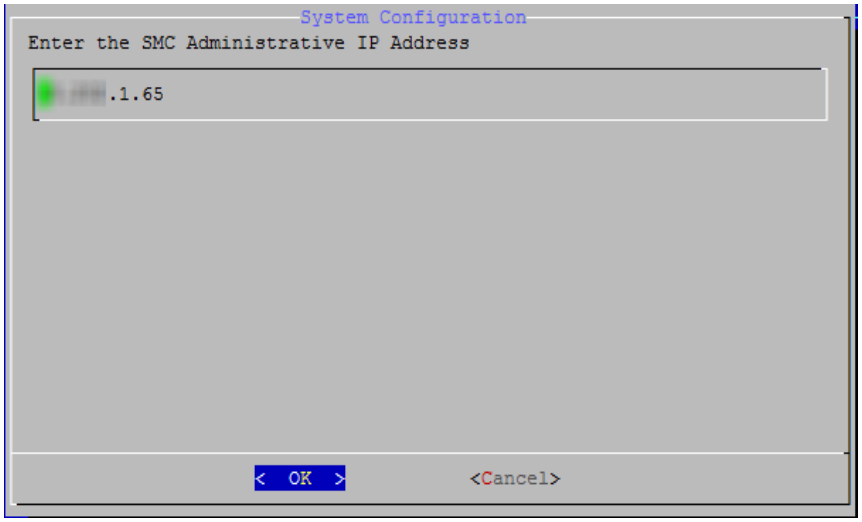
1. Inicie sessão no programa de Configuração do sistema:

   - Introduza **sysadmin** e, em seguida, prima **Enter**.
   - Quando for apresentada linha de comandos para introduzir a palavra-passe, introduza **lan1cope** e, em seguida, prima **Enter**.
   - Na linha de comandos seguinte, introduza **SystemConfig** e, em seguida, prima **Enter**.

     Abre-se o menu de Configuração do Sistema.

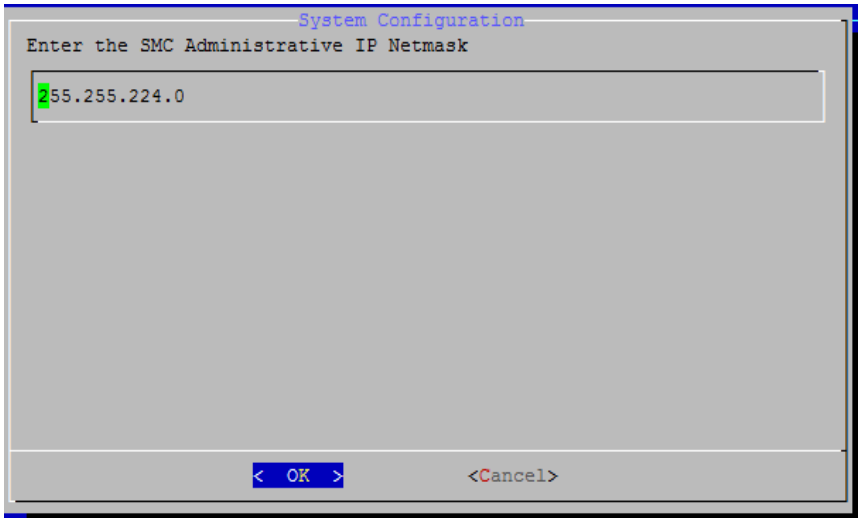


2. Selecione **Management** (Gestão) e, em seguida, prima **Enter**. Abre-se a página de endereço IP.



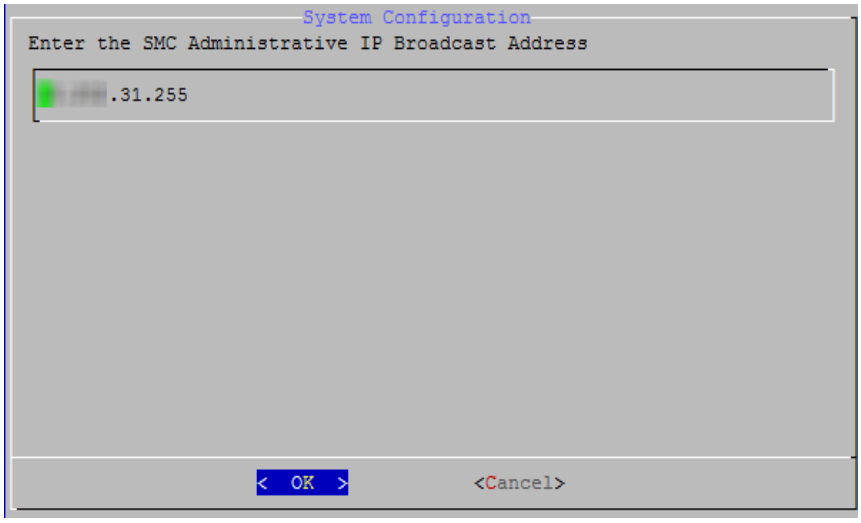
3. Introduza um novo endereço IP, com base no seu ambiente. Selecione **OK** e, em seguida, prima **Enter** para continuar.

   A página de máscara de rede IP abre-se e apresenta o valor predefinido.



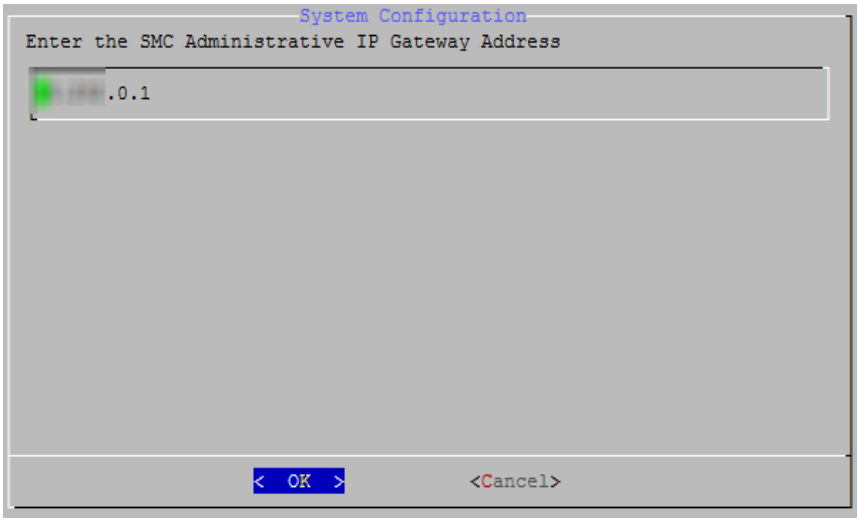
4. Aceite o valor predefinido ou introduza um novo endereço IP de máscara de rede, com base no seu ambiente. Selecione **OK** e, em seguida, prima **Enter** para continuar.

Abre-se a página Broadcast Address (Endereço de transmissão).



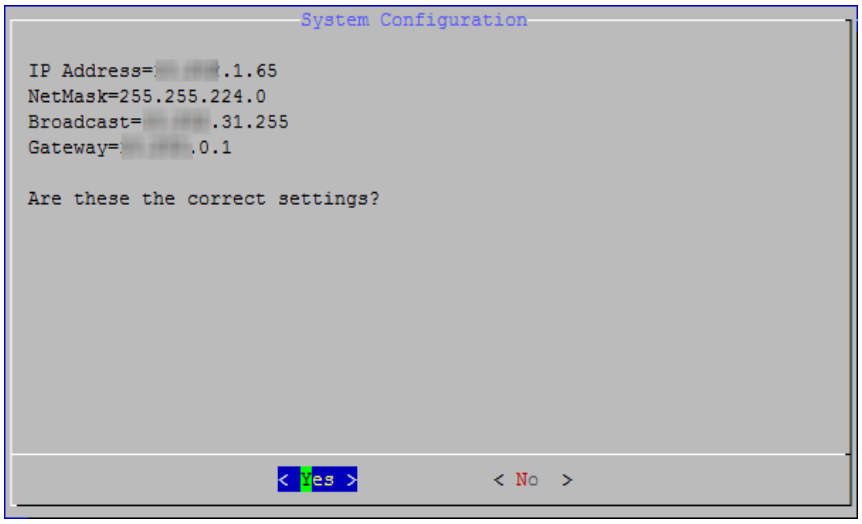
5. Aceite o valor predefinido ou introduza um novo, com base no seu ambiente. Selecione **OK** e, em seguida, prima **Enter** para continuar.

   Abre-se a página Gateway Address (Endereço do gateway) com o endereço IP do servidor de gateway predefinido.



6. Aceite o valor predefinido ou introduza um novo, com base no seu ambiente. Selecione **OK** e, em seguida, prima **Enter** para continuar.

Abre-se a página de confirmação.



7. Reveja as informações. As definições estão corretas?

- Se sim, selecione **Yes** (Sim) e, em seguida, prima **Enter** para continuar. O sistema reinicia e implementa as alterações. Depois de reiniciar, abre-se a página Login (Início de sessão).
- Se não, selecione **No** (Não) para efetuar as correções. A página de endereço IP abre-se para poder introduzir as alterações. Depois de efetuar as alterações e aceitar as definições, abre-se a página Restart (Reiniciar). Prima **Enter** para implementar as alterações.***Não me surgiu a página com a mensagem de reinício.***

8. Continue para a próxima secção, **Alteração da palavra-passe do utilizador Sysadmin**.

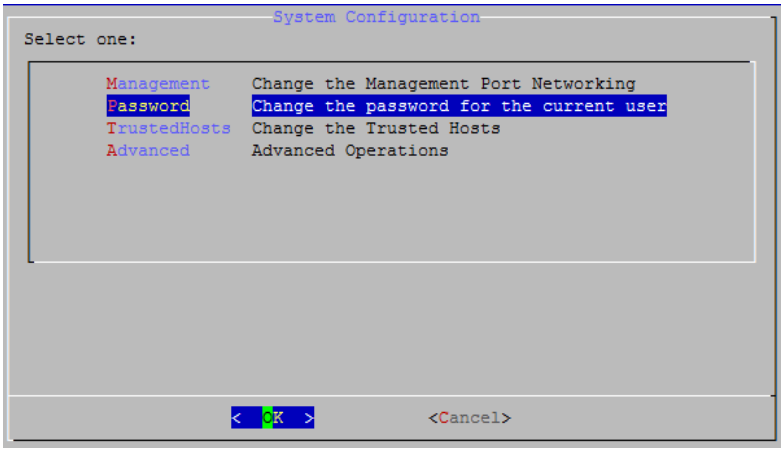
Alteração da palavra-passe do utilizador Sysadmin

Para garantir que a sua rede é segura, altere a palavra-passe predefinida para o utilizador sysadmin no dispositivos.

Certifique-se de que iniciou sessão com o utilizador **sysadmin** para iniciar este procedimento.

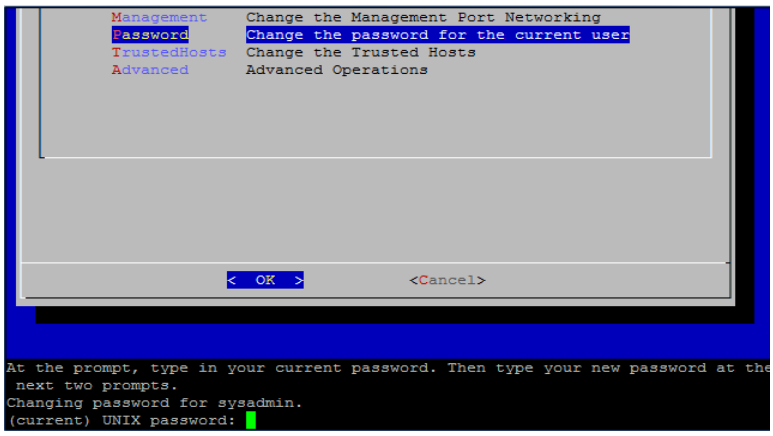
Para alterar a palavra-passe do utilizador sysadmin:

1. No menu System Configuration (Configuração do sistema), selecione **Password** (Palavra-passe) e prima **Enter**.



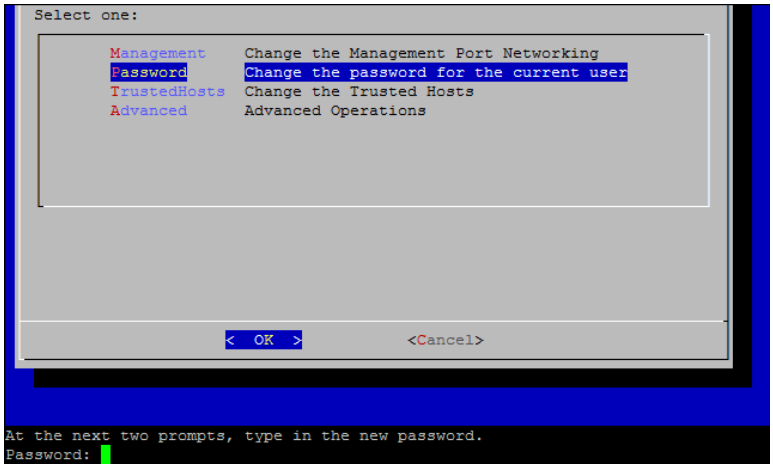
   Se alterou a lista de anfitriões fidedignos nas predefinições, certifique-se de que todos os dispositivos Stealthwatch estão incluídos nessa lista em todos os dispositivos Stealthwatch da sua implementação. Caso contrário, os dispositivos não conseguirão comunicar entre si.

   Abaixo do menu, é apresentada a linha de comandos para introduzir a palavra-passe atual.



2. Introduza a palavra-passe atual e, em seguida, prima **Enter**.

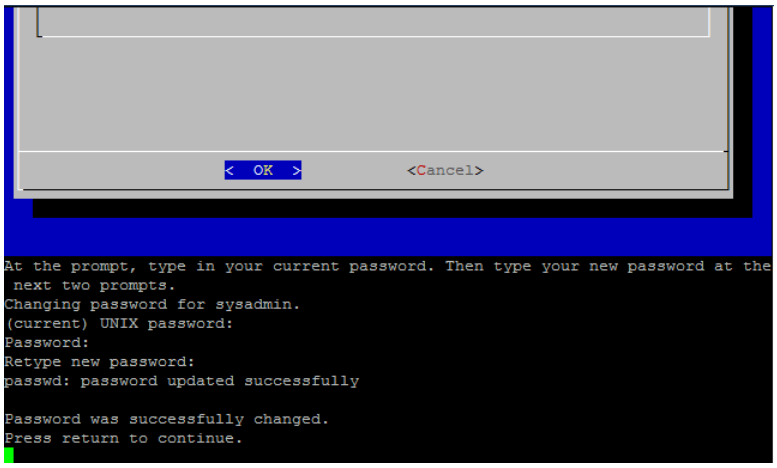
   É apresentada a linha de comandos para introduzir uma palavra-passe nova.



3. Introduza a palavra-passe nova e, em seguida, prima **Enter**.

   A palavra-passe tem de conter 8 a 30 carateres alfanuméricos e não pode conter espaços. Também pode utilizar os seguintes carateres especiais: $.~!@#%_=?:,{}()

4. Volte a introduzir a palavra-passe e, em seguida, prima **Enter**.

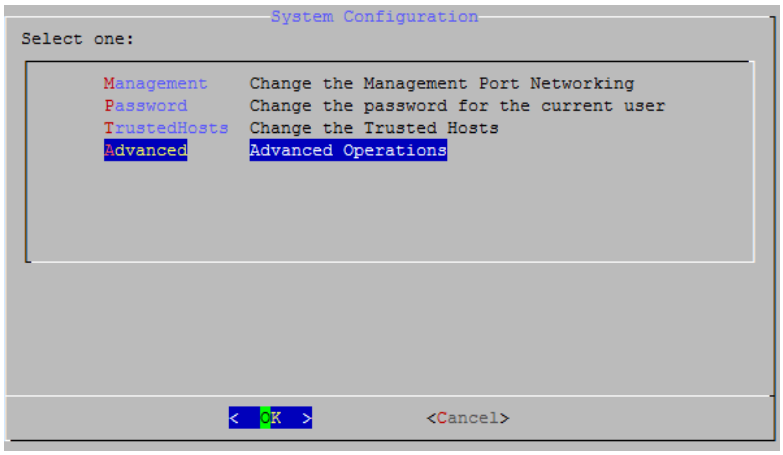


5. Quando a palavra-passe for aceite, prima **Enter** novamente para voltar ao menu System Configuration (Configuração do sistema).
6. Continue para a próxima secção, **Alteração da palavra-passe do utilizador raiz** .

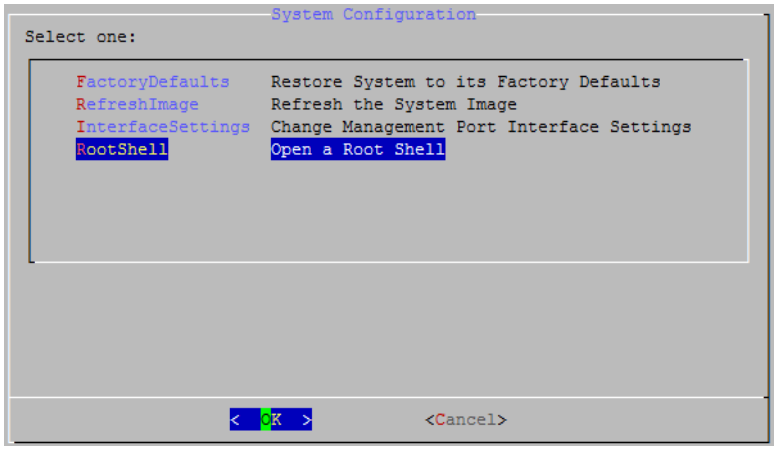
Alteração da palavra-passe do utilizador raiz

Depois de alterar a palavra-passe predefinida do utilizador sysadmin, altere a palavra-passe predefinida do utilizador raiz para proteger ainda mais a sua rede.

1. Aceda à shell raiz.

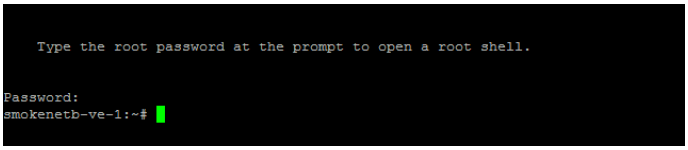


2. No menu System Configuration (Configuração do sistema), selecione **Advanced** (Avançadas) e prima **Enter**. É apresentado o menu Advanced (Avançadas).

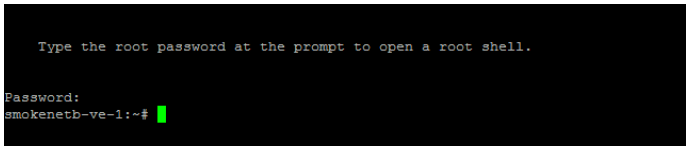


3. Selecione **RootShell** e, em seguida, prima **Enter**.

   É apresentado um pedido para introduzir uma palavra-passe do utilizador raiz.



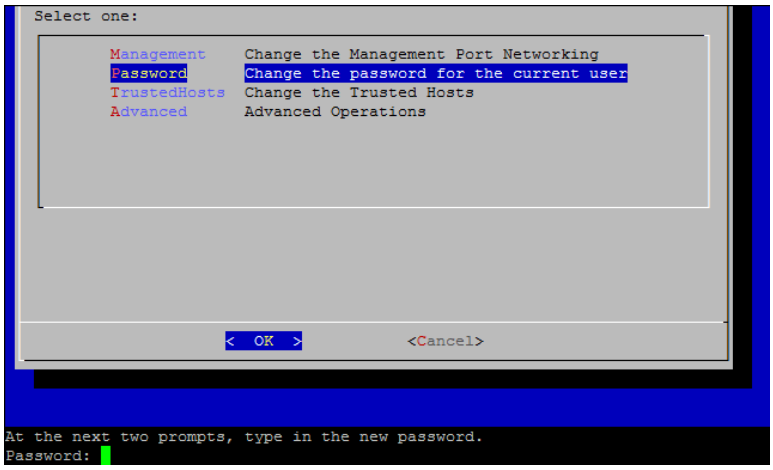
4. Introduza a palavra-passe atual do utilizador raiz e, em seguida, prima **Enter**. É apresentada a linha de comandos da shell de raiz.



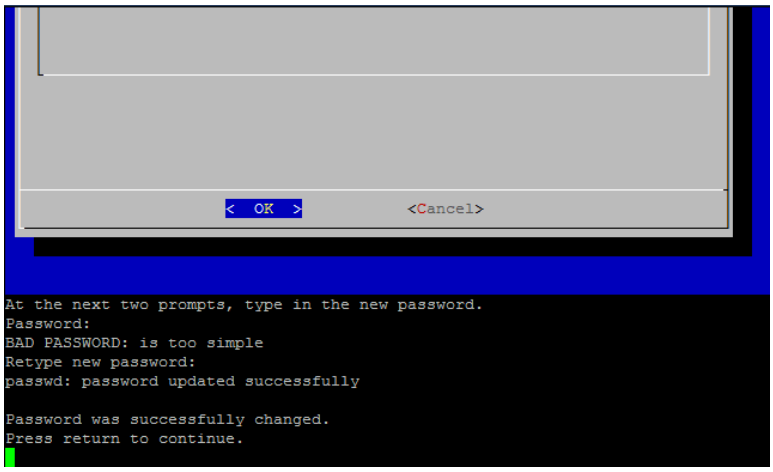
5. Introduza **SystemConfig** e, em seguida, prima **Enter**.

   Através deste comando, volta ao menu System Configuration (Configuração do sistema) para poder alterar a palavra-passe do utilizador raiz.

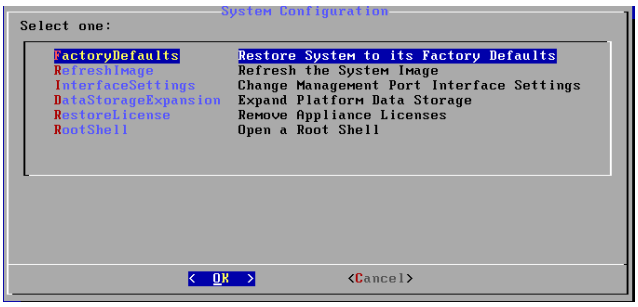
6. Selecione **Password** (Palavra-passe) e, em seguida, prima **Enter**. Abaixo do menu, é apresentada a linha de comandos para introduzir a palavra-passe.



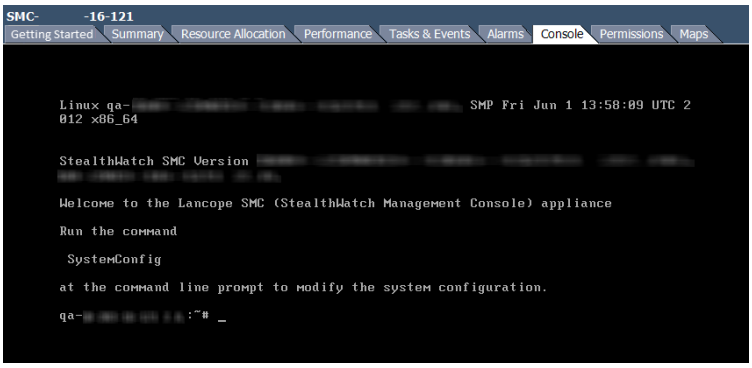
7. Introduza a palavra-passe nova do utilizador raiz e, em seguida, prima **Enter**. É apresentado um segundo pedido.



8. Volte a introduzir a palavra-passe nova do utilizador raiz e, em seguida, prima **Enter**.
9. Assim que a palavra-passe for alterada com êxito, prima **Enter**. Desta forma, atualizou as palavras-passe predefinidas dos utilizadores sysadmin e raiz. Em seguida, volta ao menu da consola System Configuration (Configuração do sistema).



10. Selecione **Cancel** (Cancelar) e prima **Enter**. A consola System Configuration (Configuração do sistema) fecha-se e é apresentada a linha de comandos da shell raiz.



11. Introduza **exit** e prima **Enter**. É apresentada a linha de comandos de início de sessão.
12. Prima **Ctrl+Alt** para sair do ambiente da consola.

Configuração do dispositivo

Agora já está tudo a postos para configurar o seu dispositivo. Para configurar o seu dispositivo, consulte o **Guia de configuração e instalação do Stealthwatch** aplicável à versão do seu software. A x210 Series é compatível com as versões 7.x do software Stealthwatch.

Copyright Information