Cisco Secure Network Analytics

Manual de Instalação do Dispositivo de Hardware Série x2xx (com Data Store)

Índice

Introdução

Descrição geral

Este guia explica como instalar os dispositivos de hardware do Cisco Secure Network Analytics (anteriormente Stealthwatch) Série x2xx. Descreve os componentes Secure Network Analytics 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 Secure Network Analytics. O hardware da Série x2xx inclui:

Dispositivo	**Número de peça**
Data Store 6200 (três Nós de dados)	ST-DS6200-K9 (três ST-DNODE-G1)
Coletor de fluxo 4210	ST-FC4210-K9
Coletor de fluxo 5210 Motor	ST-FC5210-E
Coletor de fluxo 5210 Base de dados	ST-FC5210-D
Sensor de fluxo 1210	ST-FS1210-K9
Sensor de fluxo 3210	ST-FS3210-K9
Sensor de fluxo 4240	ST-FS4240-K9
Gestor 2210 (anteriormente Consola de gestão Stealthwatch)	ST-SMC2210-K9
UDP Director 2210	ST-UDP2210-K9

Público-alvo

Este guia foi concebido para orientar a pessoa responsável pela instalação do hardware Secure Network Analytics. 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, UDP Director e o Gestor).

> Para obter informações acerca da configuração de dispositivos Secure Network Analytics, consulte o Guia de configuração do sistema **Cisco Secure Network Analytics** e o Guia de implementação e configuração do hardware do Armazenamento de dados do Cisco Secure Network Analytics aplicáveis à versão do seu software. A Série x2xx é compatível com as versões de software 7.x do Secure Network Analytics.

Como utilizar este guia

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

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

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
UPS	Fonte de alimentação ininterrupta
VLAN	Rede local virtual

Considerações relativas à pré-configuração

Esta secção examina o que deve considerar antes de instalar e configurar os seus dispositivos Secure Network Analytics. Explica onde colocar os dispositivos Secure Network Analytics e como os integrar na sua rede. Inclui:

- **Início de sessão com a palavra-passe predefinida CIMC**
- **Sobre os dispositivos Secure Network Analytics**
- **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.

- Inicie sessão no CIMC como Administrador e introduza **password** no campo Palavra-passe.
- Depois de iniciar sessão, altere a palavra-passe predefinida para garantir a segurança da sua rede.

Sobre os dispositivos Secure Network Analytics

Secure Network Analytics 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 da Série Secure Network Analytics x2xx.

> Para obter mais informações, consulte as folhas de especificações de cada dispositivo Secure Network Analytics Série x2xx.

Gestor 2210

O Gestor gere, coordena, configura e organiza todos os diferentes componentes do sistema. O software Secure Network Analytics permite-lhe aceder à IU web da consola a partir de qualquer computador com acesso a um web browser. Pode aceder facilmente a informações de segurança e de rede, em tempo real, relativas a segmentos críticos de toda a sua empresa. Com independência de plataforma baseada em Java, o Gestor permite:

- Efetuar a gestão, configuração e criação de relatórios centralizadas de até 25 coletores de fluxo Secure Network Analytics
- 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
- Efetuar a monitorização do desempenho
- Obter notificações imediatas se ocorrerem falhas de segurança

Os utilizadores que implementem um Data Store podem configurar um Gestor 2210 com uma interface SFP+ DAC de 10 Gbps como eth0 para maior débito. Os utilizadores que não implementem um Data Store apenas podem configurar a interface de cobre de 100 Mbps/1 Gbps/10 Gbps como eth0.

Coletor de fluxo 4210 e 5210

O Coletor de fluxo 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.

Os utilizadores que implementem um Data Store podem configurar um Coletor de fluxo 4210 com uma interface SFP+ DAC de 10 Gbps como eth0 para maior capacidade. Os utilizadores que não implementem um Data Store apenas podem configurar a interface de cobre de 100 Mbps/1 Gbps/10 Gbps como eth0.

> 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 Secure Network Analytics identifica o comportamento, o sistema pode tomar quaisquer medidas que tenha configurado em relação a qualquer tipo de comportamento.

Data Store 6200

O Data Store oferece um repositório central para armazenar a telemetria da sua rede, recolhida pelos seus Coletores de fluxo. O Data Store é composto por um cluster de Nós de dados, cada um contendo uma parte dos seus dados, e por uma cópia de segurança de dados de um Nó de dados separado. Como todos os seus dados estão numa base de dados centralizada e não espalhados por vários Coletores de fluxo, o seu Gestor pode

obter resultados de consulta a partir do Data Store mais rapidamente do que se consultasse todos os seus Coletores de fluxo separadamente. O Data Store oferece melhor tolerância a falhas, melhor resposta de consulta e um preenchimento mais rápido de gráficos e tabelas.

Sensor de fluxo 1210, 3210 e 4240

O Sensor de fluxo 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 um 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 Secure Network Analytics, 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.

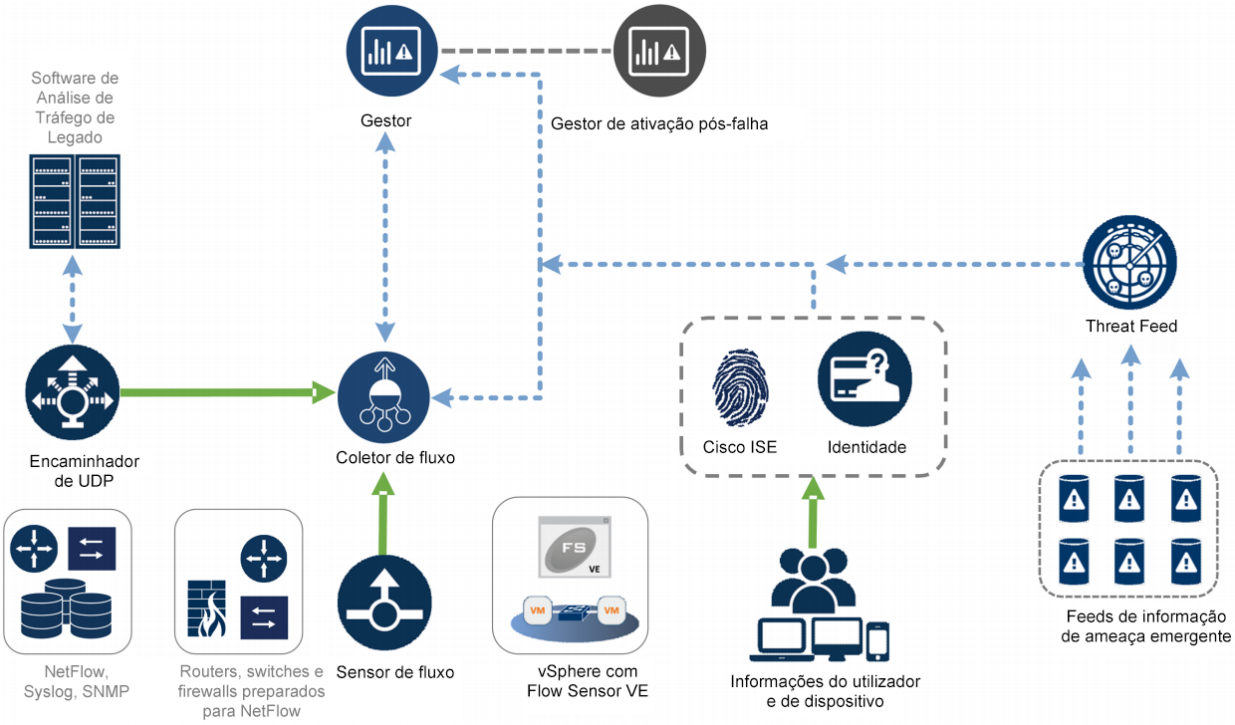
Encaminhador de UDP 2210

O Encaminhador de UDP 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 Secure Network Analytics 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 do Gestor

Instale o Gestor como dispositivo de gestão numa localização da sua rede que seja acessível a todos os dispositivos que enviam dados para o mesmo.

Se tiver o par de ativação pós-falha de Gestores, recomenda-se que instale os Gestores primário e secundário em localizações físicas separadas. Esta estratégia otimiza qualquer esforço de recuperação de desastres, caso seja necessário.

Posicionamento do Coletor de fluxo

Enquanto dispositivo de recolha e monitorização, o Coletor de fluxo 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

Enquanto dispositivo de monitorização passiva, o Sensor de fluxo 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 root
- 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)

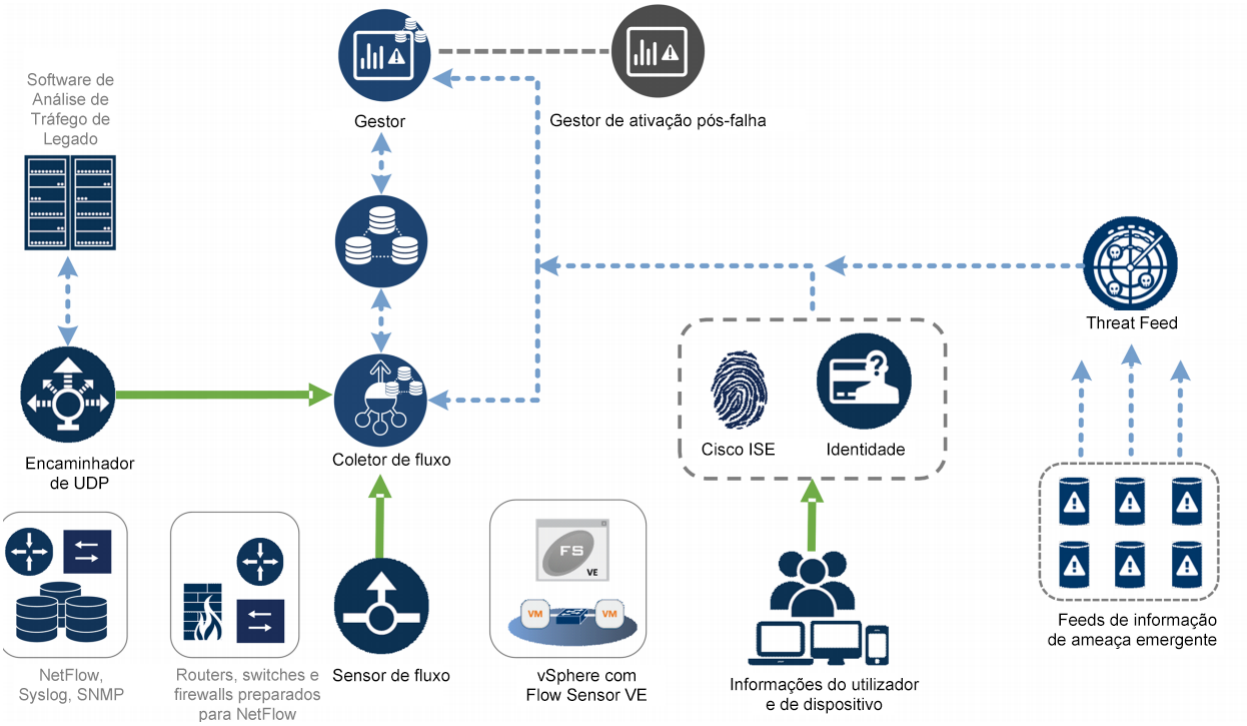
Posicionamento do Encaminhador de UDP

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

⚠ Se implementar o Encaminhador de UDP num ambiente em que esteja a ser utilizado o ACI da Cisco e o Unicast Reverse Path Forwarding (uRPF) ou **Limit IP learning to subnet** estiver ativado, a rede local pode bloquear o tráfego encaminhado que sai do Encaminhador de UDP. Tem de fazer o spoofing do tráfego do UDP como parte das regras de encaminhamento para que as ferramentas que recolhem os dados de registo possam conhecer a fonte original do tráfego.

Para garantir um funcionamento com sucesso do Encaminhador de UDP neste caso, utilize o seu Encaminhador de UDP numa parte da sua rede em que possa desativar o uRPF ou **Limit IP learning to subnet** (tipicamente, internamente). Pode posicionar o Encaminhador de UDP num L3 out (sem aprendizagem de IP). Se estiver em 4.0+, pode desativar a aprendizagem de ponto final numa base VRF.

O diagrama seguinte apresenta uma implementação de Secure Network Analytics com um Data Store.

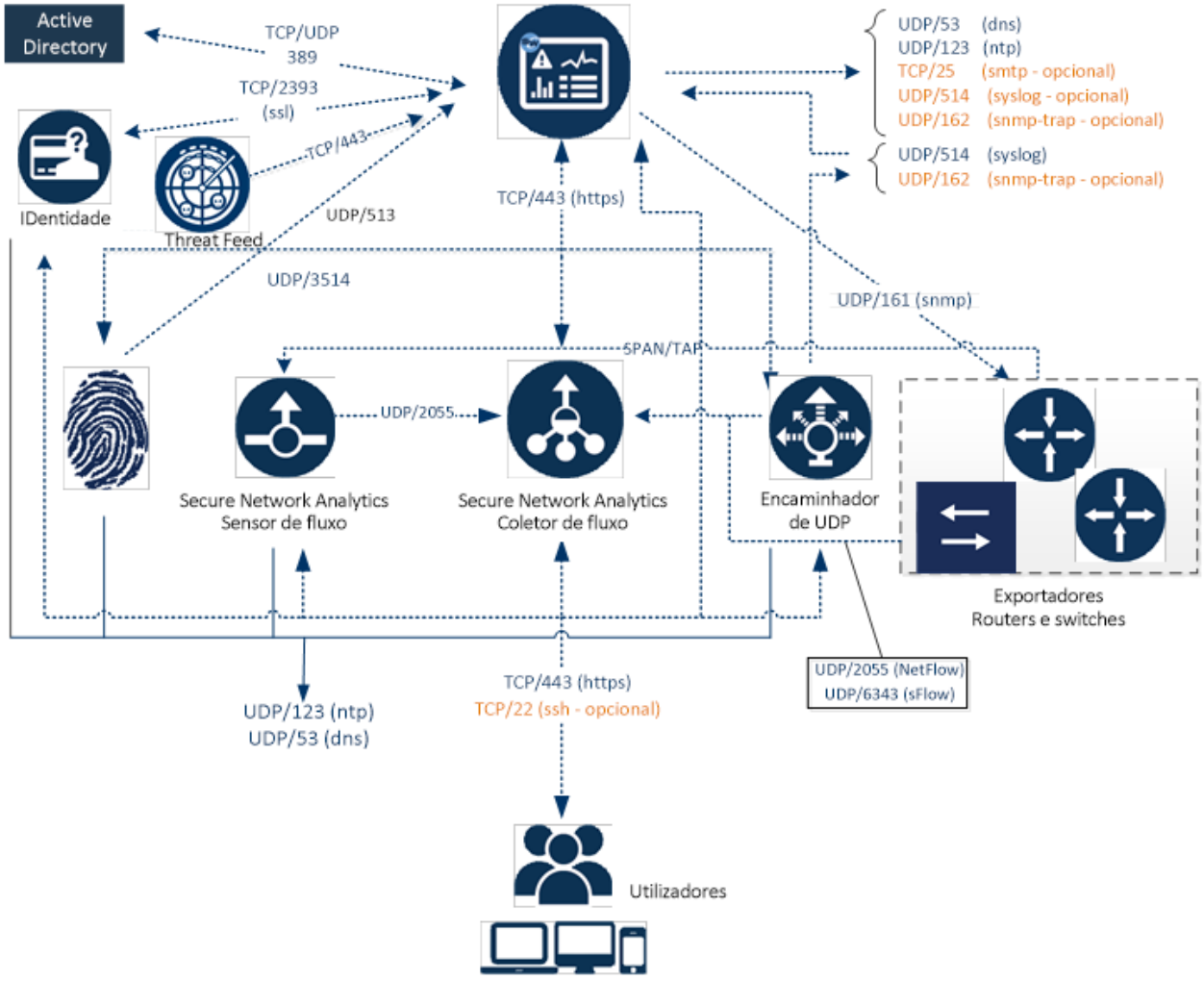


Posicionamento do Data Store Secure Network Analytics

Como repositório para dados de fluxo recolhidos pelos Coletores de fluxo e como repositório centralizado com o qual um Gestor realiza consultas, instale os seus Nós de dados num local da sua rede acessível a todos os seus Coletores de fluxo e ao Gestor. Consulte o Guia de implementação e configuração do hardware do Data Store para mais informações.

Portas de comunicação

O diagrama seguinte apresenta portas de comunicação para abrir na sua implementação de Secure Network Analytics.



A tabela seguinte indica como são utilizadas as portas no Secure Network Analytics:

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

De (Cliente)	Para (Servidor)	Porta	Protocolo
Active Directory	Gestor	TCP/389, UDP/389	LDAP
Cisco ISE	Gestor	TCP/443	HTTPS
Cisco ISE	Gestor	TCP/8910	XMPP
Origens de registo externas	Gestor	UDP/514	SYSLOG
Coletor de fluxo	Gestor	TCP/443	HTTPS
Threat Feed	Gestor	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
Sensor de fluxo	Gestor	TCP/443	HTTPS
Sensor de fluxo	Coletor de fluxo - NetFlow	UDP/2055	NetFlow
Identidade	Gestor	TCP/2393	SSL
Exportadores NetFlow	Coletor de fluxo - NetFlow	UDP/2055*	NetFlow
Exportadores sFlow	Coletor de fluxo - sFlow	UDP/6343*	sFlow
Gestor	Cisco ISE	TCP/443	HTTPS

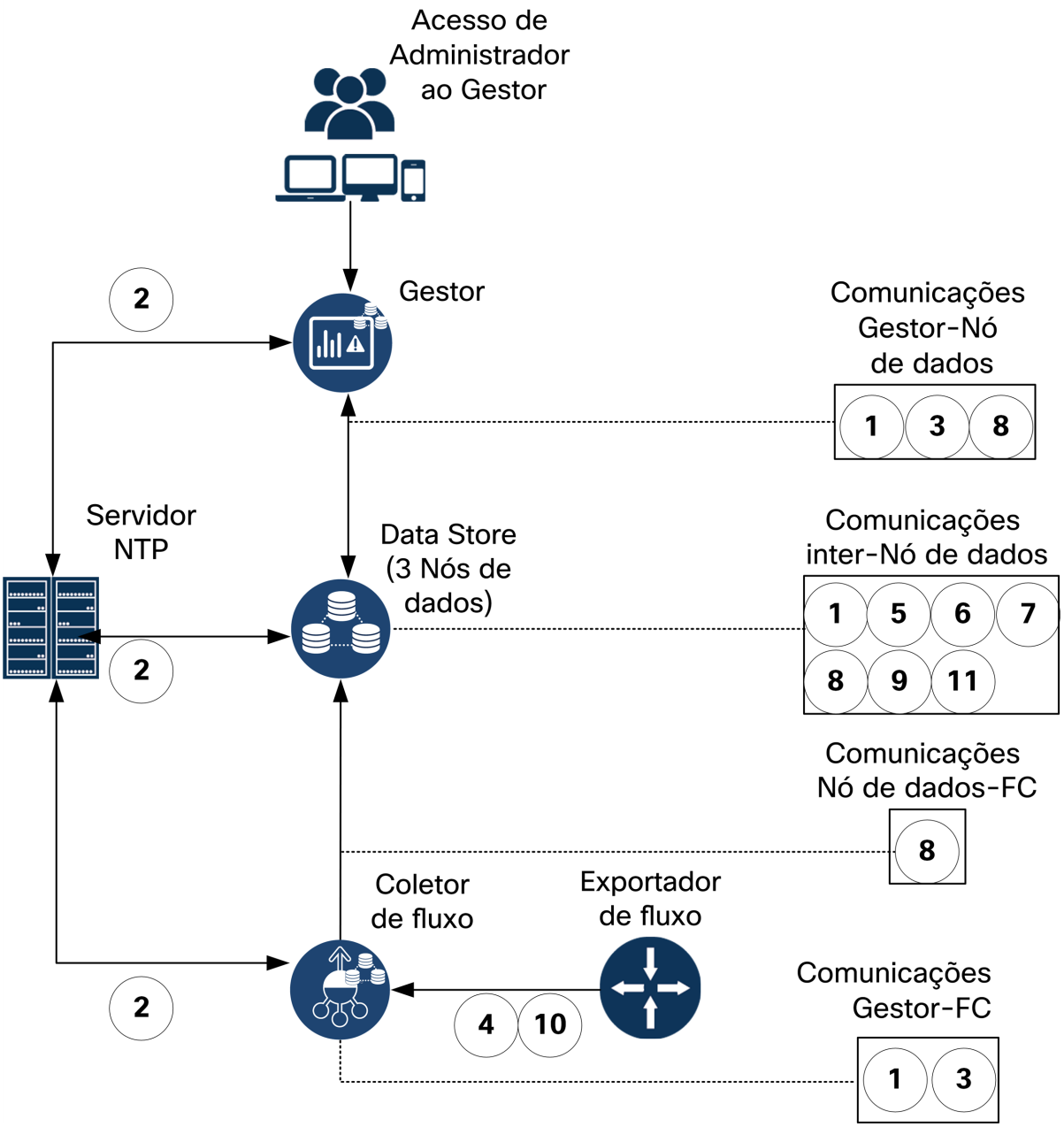
De (Cliente)	Para (Servidor)	Porta	Protocolo
Gestor	DNS	UDP/53	DNS
Gestor	Coletor de fluxo	TCP/443	HTTPS
Gestor	Sensor de fluxo	TCP/443	HTTPS
Gestor	Identidade	TCP/2393	SSL
Gestor	Exportadores de fluxo	UDP/161	SNMP
PC do utilizador	Gestor	TCP/443	HTTPS

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

A tabela seguinte indica as configurações opcionais determinadas pelos seus requisitos de administração de rede:

De (Cliente)	Para (Servidor)	Porta	Protocolo
Todos os dispositivos	PC do utilizador	TCP/22	SSH
Gestor	Gestão de eventos de terceiros	UDP/162	SNMP-trap
Gestor	Gestão de eventos de terceiros	UDP/514	SYSLOG
Gestor	Gateway de e-mail	TCP/25	SMTP
Gestor	Threat Feed	TCP/443	SSL
PC do utilizador	Todos os dispositivos	TCP/22	SSH

O diagrama seguinte apresenta portas adicionais a abrir se implementar um Data Store na sua rede:



A tabela seguinte inclui portas utilizadas se implementar um Data Store na sua rede:

#	De (Cliente)	Para (Servidor)	Porta	Protocolo ou Finalidade
1	Gestor	Coletores de fluxo e Nós de dados	22/TCP	SSH, necessário para inicializar a base de dados do Data Store

1	Nós de dados	todos os outros Nós de dados	22/TCP	SSH, necessário para inicializar a base de dados do Data Store e para tarefas de administração da base de dados
2	Gestor Coletores de fluxo e Nós de dados	Servidor NTP	123/UDP	NTP, necessário para sincronização de tempo
2	Servidor NTP	Gestor Coletores de fluxo e Nós de dados	123/UDP	NTP, necessário para sincronização de tempo
3	Gestor	Coletores de fluxo e Nós de dados	443/TCP	HTTPS, necessário para comunicações seguras entre aplicações
3	Coletores de fluxo	Gestor	443/TCP	HTTPS, necessário para comunicações seguras entre aplicações
3	Nós de dados	Gestor	443/TCP	HTTPS, necessário para comunicações seguras entre aplicações
4	Exportadores NetFlow	Coletor de fluxo (NetFlow)	2055/UDP	Ingestão NetFlow
5	Nós de dados	todos os outros Nós de dados	4803/TCP	Serviço de mensagens inter-Nó de dados
6	Nós de dados	todos os outros Nós de dados	4803/UDP	Serviço de mensagens inter-Nó de dados

7	Nós de dados	todos os outros Nós de dados	4804/UDP	Serviço de mensagens inter-Nó de dados
8	Gestor Coletores de fluxo e Nós de dados	Nós de dados	5433/TCP	Ligações de cliente Vertica
9	Nó de dados	todos os outros Nós de dados	5433/UDP	Monitorização do serviço de mensagens Vertica
10	Exportadores sFlow	Coletor de fluxo (sFlow)	6343/UDP	Ingestão sFlow
11	Nós de dados	todos os outros Nós de dados	6543/UDP	Serviço de mensagens inter-Nó de dados

Integração do Sensor de fluxo na sua rede

O Sensor de fluxo 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 pretende 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 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.

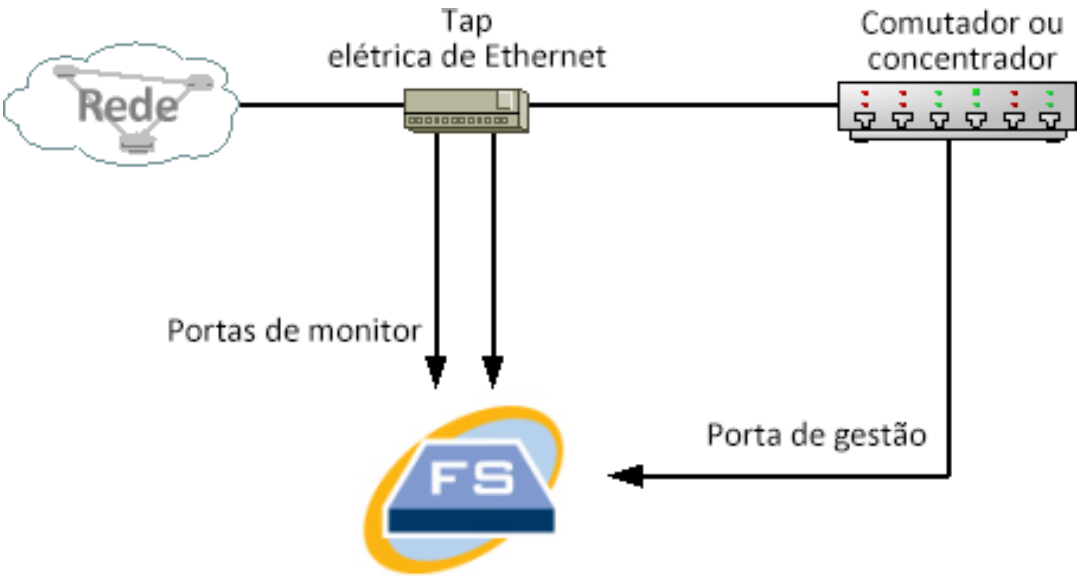
Esta secção explica as seguintes formas de utilizar TAPs:

- **Utilizar TAPs elétricas**
- **Utilizar TAPs óticas**
- **Utilizar TAPs fora da sua firewall**
- **Colocar o Sensor de fluxo 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

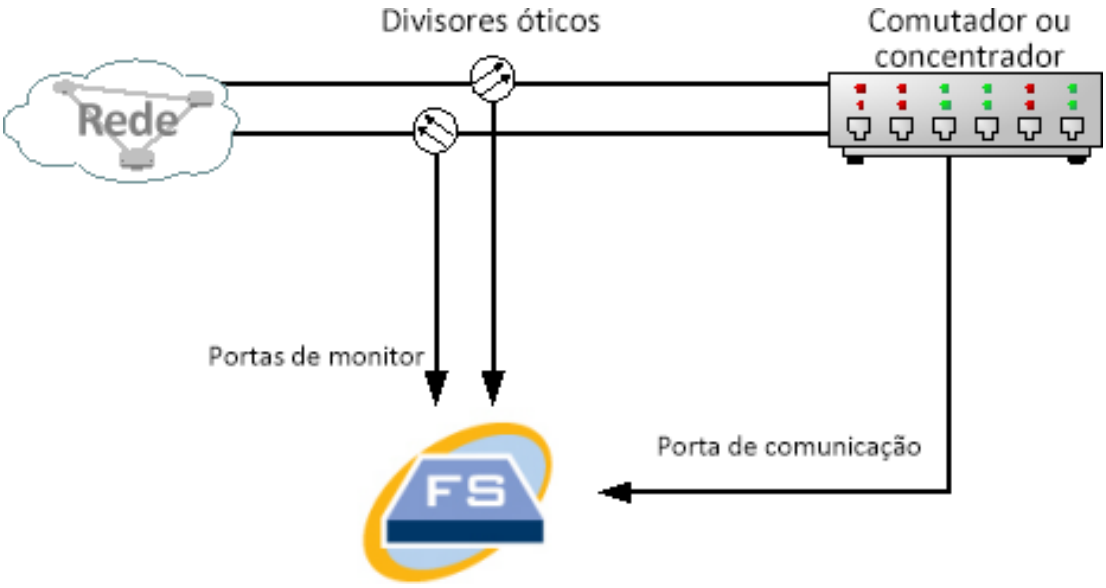
No exemplo abaixo, o Sensor de fluxo está ligado a uma TAP de Ethernet elétrica. Para tal, ligue as duas portas TAP às portas Monitor 1 e 2 do Sensor de fluxo.



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.



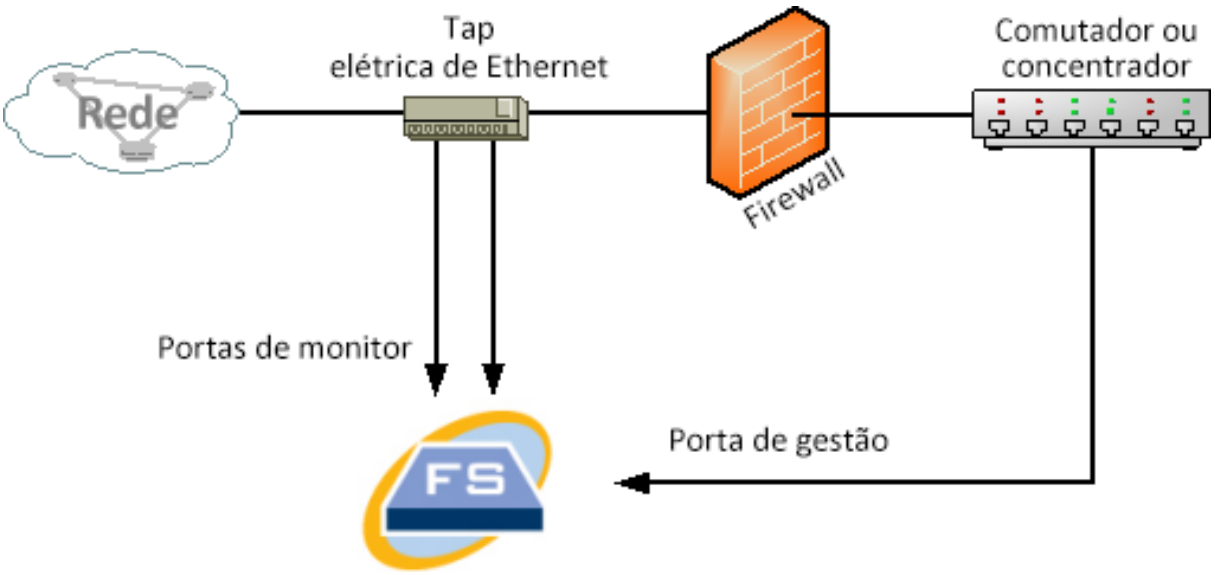
Se existir uma ligação de fibra ótica entre as redes monitorizadas, o Sensor de fluxo é ligado a dois divisores óticos. A porta de gestão é ligada ao switch da rede monitorizada ou a outro switch ou hub.

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 Secure Network Analytics 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.

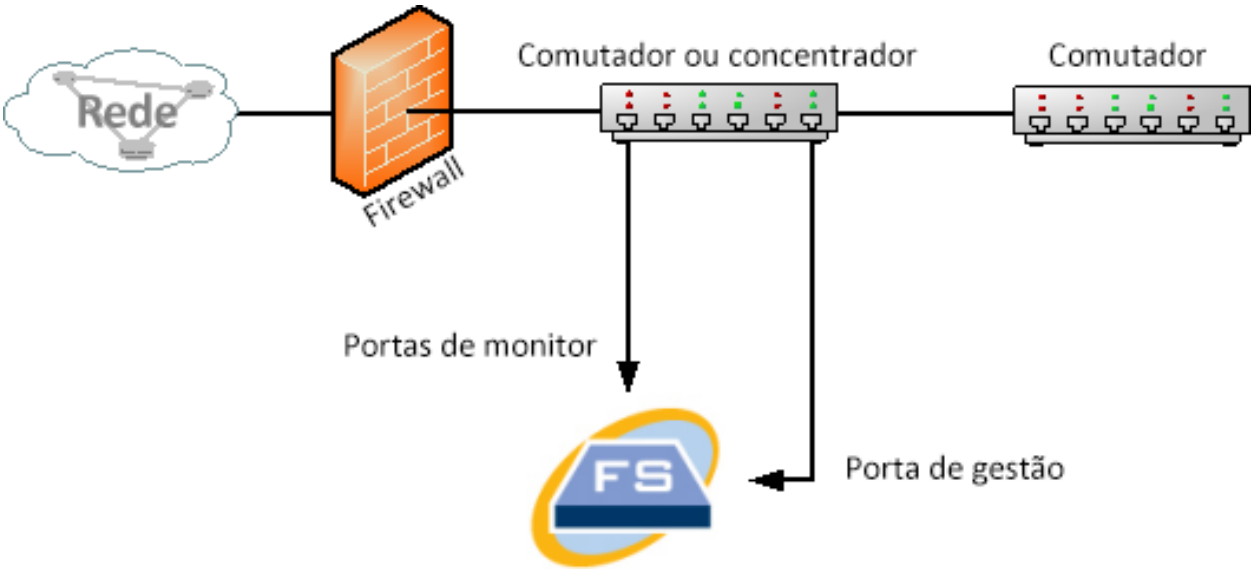
O exemplo abaixo mostra a utilização de uma TAP de Ethernet elétrica. A porta de gestão tem de ser ligada ao switch ou ao hub da rede monitorizada. Esta configuração é semelhante à configuração que monitoriza o tráfego enviado e recebido pela sua rede.



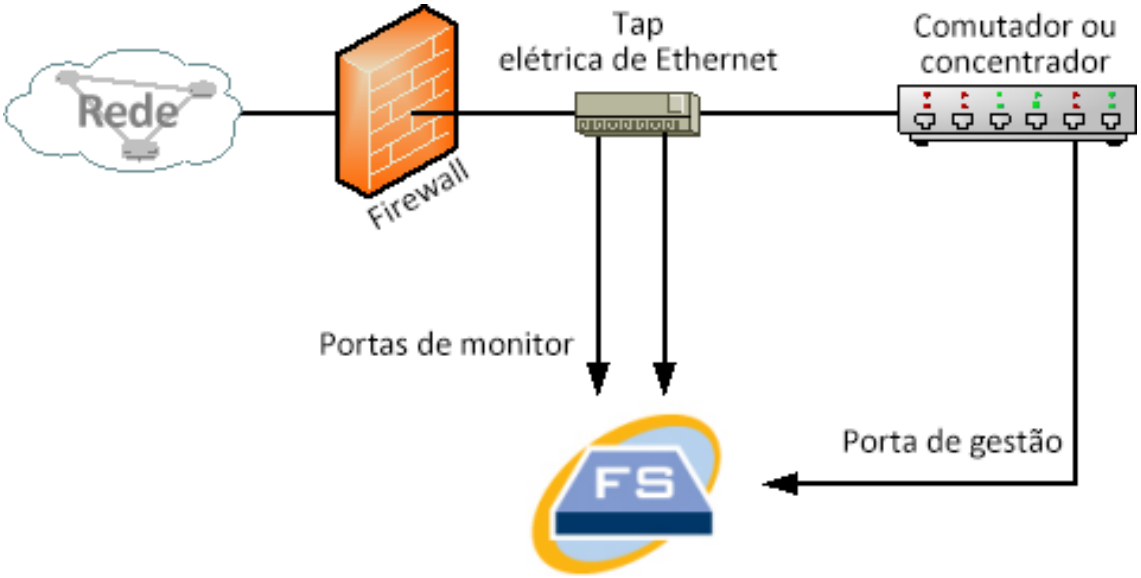
Se a sua firewall estiver a executar a tradução de endereços de rede (NAT), apenas pode observar os endereços que estão na firewall.

Colocar o Sensor de fluxo dentro da firewall

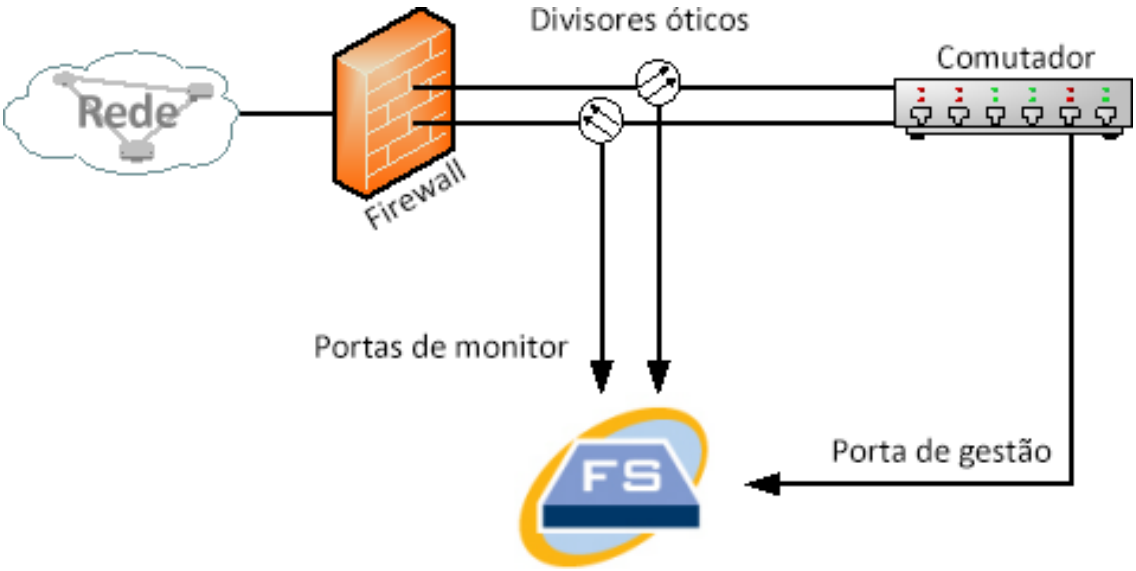
Para monitorizar o tráfego entre redes internas e uma firewall, o Sensor de fluxo tem de poder aceder a todo o tráfego entre a firewall e as redes internas. Para tal, configure uma porta de espelhamento que replique a ligação à firewall no switch principal. Certifique-se de que a porta Monitor 1 do Sensor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



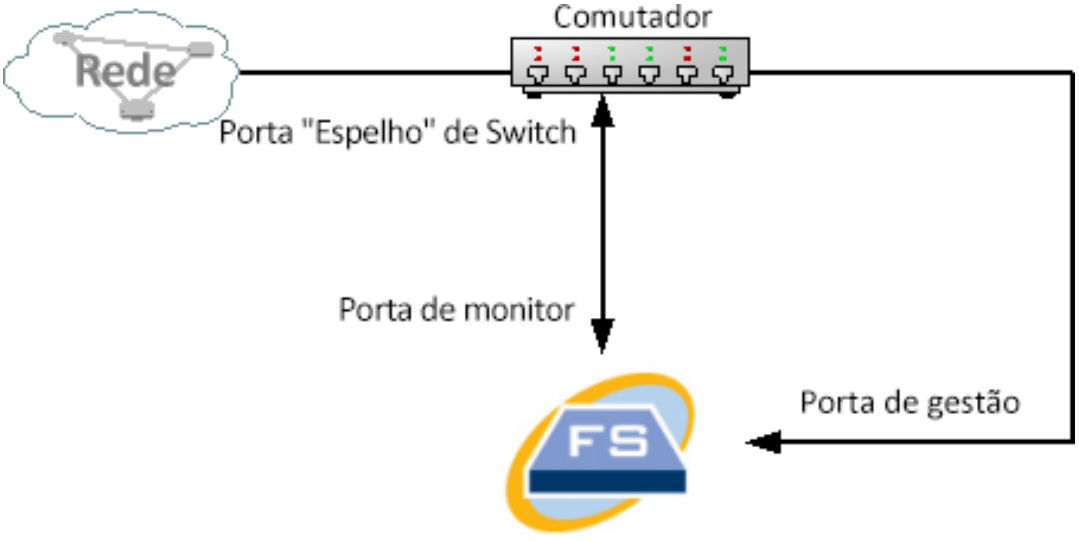
A configuração do divisor ótico é apresentada abaixo.



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 Secure Network Analytics 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 todo 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 a porta de espelhamento.

Preparação da instalação

Avisos relativos à instalação

Leia o documento Informações de segurança e conformidade regulamentar antes de instalar os dispositivos Secure Network Analytics da série x2xx.

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 joias

Antes de trabalhar em equipamento ligado à eletricidade, retire todas as joias 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 35 °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 o 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 joias, 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 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 rack não bloqueia as portas de admissão e de exaustão se estiver a montar um chassi num bastidor aberto.
- Assegure que os racks fechados possuem uma ventilação adequada. Certifique-se de que o racknão está demasiado congestionado, já que cada chassi produz calor. Os racks fechados devem ter laterais em persiana e uma ventoinha para fornecer ar de ventilação.
- Num rack fechado com uma ventoinha de ventilação na parte superior, o calor produzido pelo equipamento próximo da parte inferior do rack pode ser puxado para cima e para dentro das portas de admissão do equipamento que se encontra por cima, no rack. Assegure uma ventilação adequada no equipamento na parte inferior do rack.
- 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 rack. Experimente diferentes disposições para posicionar os defletores da forma mais eficaz.

Instalação de hardware

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

- **Montagem do dispositivo**
- **Ligação do dispositivo à rede**
- **Ligação do dispositivo**
- **Configurar as definições de rede utilizando a Configuração inicial**

Montagem do dispositivo

Pode montar os dispositivos Secure Network Analytics 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 CA condicionada
- O fluxo de ar em torno do dispositivo e no interior das condutas não apresente restrições.

Hardware incluído com o dispositivo

Os dispositivos Secure Network Analytics 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.

> ⚠ Não atualize o dispositivo BIOS, pois pode provocar problemas na funcionalidade do dispositivo.

Para obter informações detalhadas relativas às especificações, consulte as Folhas de especificações do Secure Network Analytics.

> ⓘ Todo o hardware Cisco x2xx 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 **Configurar as definições de rede utilizando a Configuração inicial**.

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, **Configurar as definições de rede utilizando a Configuração inicial**.

Configurar as definições de rede utilizando a Configuração inicial

Após se ligar ao dispositivo, utilize a Configuração inicial para configurar as definições de rede, incluindo endereços IP. Lembre-se do seguinte:

- Se implementar um Gestor 2210 ou Coletor de fluxo 4210 com um Data Store, além de configurar os endereços IP, pode também configurar o Gestor ou Coletor de fluxo para utilização do Data Store e o tipo de porta física que utiliza para a porta de gestão `eth0`.

  > ⚠ Se optar por configurar o seu Gestor ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção apenas se planear implementar um Data Store na sua rede.

- Se o seu dispositivo for um Nó de dados, pode configurar o tipo de porta física que este utiliza para a porta de gestão `eth0` e o endereço IP e informação relacionada para o canal de porta `eth2` ou `eth2`/`eth3` para comunicações do Nó de dados.

Consulte o Guia de implementação e configuração do hardware do Data Store Secure Network Analytics para mais informações sobre a instalação dos dispositivos Gestor 2210, FC 4210 e Nó de dados.

Após configurar os endereços IP e portas, altere as palavras-passe de utilizador.

> Na primeira vez que entrar na Configuração do sistema, o assistente de Configuração inicial abre-se e guia-o ao longo da configuração inicial do dispositivo. Se sair da Configuração inicial antes de concluir o assistente, na próxima vez que entrar na Configuração inicial, o assistente de Configuração inicial abre-se novamente.

Com base no seu dispositivo, aceda à secção seguinte:

- **Dispositivos compatíveis com Data Store (Gestor 2210, FC 4210)**
- **Configuração geral de dispositivo Secure Network Analytics**
- **Configuração de Nó de dados**

Configuração geral de dispositivo Secure Network Analytics

Para todos os dispositivos exceto Nós de dados, o Gestor 2210 e FC 4210, a Configuração inicial apresentada é a seguinte:

- Configurar o endereço IP e a informação de gestão do dispositivo

Configure o endereço IP e a informação de gestão do dispositivo:

Na Configuração inicial, pode configurar o endereço IP de gestão eth0 e informação relacionada do dispositivo. Para a maior parte dos dispositivos, esta é a primeira configuração na Configuração inicial.

Antes de começar

- Se estiver a configurar um Nó de dados, aceda a Configuração de Nó de dados.
- Se estiver a configurar um Gestor ou Coletor de fluxo compatível com Data Store, aceda a Dispositivos compatíveis com Data Store (Gestor 2210, FC 4210).
- Se estiver a configurar qualquer outro dispositivo Secure Network Analytics, comece pelo passo 1.

Procedimento

1. Inicie sessão no programa de Configuração do sistema:
    - Se estiver a configurar um dispositivo compatível com Data Store ou Nó de dados, digite `root` e prima **Enter**. Se estiver a configurar qualquer outro dispositivo, digite `sysadmin` e prima **Enter**.

> São necessárias permissões de `root` para configurar corretamente o Data Store e a compatibilidade do Data Store.

- Quando for apresentada a 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**.

2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial.

   Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.
3. Introduza um **endereço IP** para este dispositivo.
4. Introduza a **máscara de sub-rede** da rede.
5. Introduza um endereço de **Gateway** para o endereço IP deste dispositivo.
6. Introduza um endereço de **Difusão** para o dispositivo.
7. Introduza um **Nome de anfitrião** para o seu dispositivo.
8. Introduza um **Domínio** para o seu dispositivo.
9. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

   Esta é a última opção de configuração na Configuração inicial. O seu dispositivo reinicia e implementa as alterações. Depois de reiniciar, abre-se a página Login (Início de sessão).

O que fazer a seguir

- Altere as palavras-passe de utilizador. Consulte **Alteração da palavra-passe do utilizador Sysadmin** para obter mais informações.

Dispositivos compatíveis com Data Store (Gestor 2210, FC 4210)

Para o Gestor 2210 e FC 4210, a Configuração inicial apresentada é a seguinte:

1. Configurar a porta física de gestão eth0
2. Configurar o endereço IP e a informação de gestão do dispositivo
3. Configurar a compatibilidade do Data Store
4. Configurar a utilização do Security Analytics and Logging On Prem

Configurar a porta física de gestão eth0

Se configurar um Gestor ou Coletor de fluxo compatível com Data Store e implementar um Data Store, pode, opcionalmente, configurar `eth0` como uma porta SFP+ DAC em vez da porta de cobre BASE-T predefinida. Para estes dispositivos, esta é a primeira configuração na Configuração inicial.

Antes de começar

- Se estiver a configurar um Nó de dados ou um Gestor ou Coletor de fluxo compatível com Data Store, consulte a folha de especificações do dispositivo Secure Network Analytics relativa ao seu dispositivo para informações sobre as portas SFP+ e BASE-T suportadas.
- Se estiver a configurar um Nó de dados, aceda a Configuração de Nó de dados.
- Se estiver a configurar qualquer outro dispositivo Secure Network Analytics além de dispositivos compatíveis com Data Store, consulte Configuração geral de dispositivo Secure Network Analytics.

Procedimento

1. Inicie sessão no programa de Configuração do sistema:
   - Digite **root** e, em seguida, prima **Enter**.

     São necessárias permissões de `root` para configurar corretamente a compatibilidade do Data Store.
   - Quando for apresentada a 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**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial e apresentada a configuração de Ordem de portas. Avance para o passo 5.

   Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.
3. A partir do menu Configuração do sistema, selecione **Rede** e, em seguida, prima **Enter**.
4. Selecione **Ordem de portas** e prima Enter.

5. Tem as seguintes opções:
    - Selecione **LOM** para configurar o seu dispositivo para utilizar uma porta de cobre BASE-T para eth0.
    - Selecione **SFP+** para configurar o seu dispositivo para utilizar uma porta de fibra SFP+ para eth0.
6. Selecione **OK** para confirmar a sua seleção.

O que fazer a seguir

- Configure o endereço IP e a informação de gestão da porta de gestão eth0. Consulte o procedimento seguinte.

Configure o endereço IP e a informação de gestão do dispositivo:

Na Configuração inicial, pode configurar o endereço IP de gestão eth0 e informação relacionada do dispositivo. Para dispositivos compatíveis com Data Store, esta configuração ocorre após configurar a porta de gestão física eth0.

Antes de começar

- Se estiver a configurar um Gestor ou Coletor de fluxo compatível com Data Store, após configurar a Ordem de portas, o assistente de Configuração inicial apresenta a configuração de gestão `eth0`. Avance para o passo 3.

Procedimento

1. Inicie sessão no programa de Configuração do sistema:
    - Se estiver a configurar um dispositivo compatível com Data Store, digite `root` e prima **Enter**.

      > São necessárias permissões de `root` para configurar corretamente o Data Store e a compatibilidade do Data Store.

    - Quando for apresentada a 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**.

2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial.

   Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.
3. Introduza um **endereço IP** para este dispositivo.
4. Introduza a **máscara de sub-rede** da rede.
5. Introduza um endereço de **Gateway** para o endereço IP deste dispositivo.
6. Introduza um endereço de **Difusão** para o dispositivo.
7. Introduza um **Nome de anfitrião** para o seu dispositivo.
8. Introduza um **Domínio** para o seu dispositivo.
9. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

O que fazer a seguir

- Configure o dispositivo para utilizar sem um Data Store. Consulte o procedimento seguinte para obter mais informações.

Configurar a utilização do Data Store

Configure o seu Gestor 2210 ou FC 4210 para funcionar com um Data Store. Os seus Coletores de fluxo serão ligados a um Data Store e o seu Gestor irá consultar o Data Store.

> ⚠ Se optar por configurar o seu Gestor ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção **apenas se** planear implementar um Data Store na sua rede.

> ⓘ Tem de configurar todos os seus Gestores e Coletores de fluxo para utilização com um Data Store se implementar um Data Store. Não pode configurar alguns dos seus Coletores de fluxo para ligação ao Data Store e outros para ligação direta ao Gestor.

Antes de começar

- Se estiver na Configuração inicial, a Configuração do sistema apresenta a configuração do Data Store após terminar a configuração do endereço IP do dispositivo. Avance para o passo 3.

Procedimento

1. A partir do menu de Configuração do Sistema, selecione **Avançadas** e prima **Enter**.
2. Selecione **Data Store** e prima Enter.
3. Selecione **Sim** para configurar o seu dispositivo para compatibilidade com um Data Store.

   > ⚠ Se optar por configurar o seu Gestor ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção **apenas se** planear implementar um Data Store na sua rede.

4. Selecione **OK** para confirmar a sua seleção.

O que fazer a seguir

- Configure Security Analytics and Logging On Prem. Consulte o procedimento seguinte para obter mais informações.

Configurar a utilização do Security Analytics and Logging On Prem

Configure o seu Gestor 2210 ou FC 4210 para Security Analytics and Logging On Prem, de modo a utilizar a implementação do Secure Network Analytics para armazenar informações de eventos do Firepower. O Coletor de fluxo irá ingerir informações de eventos do Firepower e enviá-las para o Data Store para armazenamento. Posteriormente, pode consultar estas informações de eventos do Firepower a partir do Gestor ou do Centro de Gestão Firepower.

Se configurar o Security Analytics and Logging On Prem, terá também de instalar a aplicação Security Analytics and Logging On Prem no Gestor. Consulte Security Analytics and Logging: Guia de integração de eventos Firepower para obter mais informações.

> ⚠ Se optar por configurar o Gestor ou o Coletor de fluxo para utilização com o Security Analytics and Logging On Prem, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção **apenas se** planear utilizar o Secure Network Analytics para Security Analytics and Logging On Prem para armazenar as suas informações de eventos do Firepower.

Antes de começar

- Se estiver na Configuração inicial, a Configuração do sistema apresenta a configuração do Security Analytics and Logging On Prem após terminar a configuração da utilização do Data Store.

Procedimento

1. Selecione **Sim** para ativar o Security Analytics and Logging On Prem e ingerir informações de eventos de firewall da sua implementação do Firepower. Note que isto desativa a recolha NetFlow no seu Coletor de fluxo.

   > ⚠ Se optar por configurar o Gestor ou o Coletor de fluxo para utilização com o Security Analytics and Logging On Prem, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção **apenas se** planear utilizar o Secure Network Analytics para Security Analytics and Logging On Prem para armazenar as suas informações de eventos do Firepower.

2. Selecione **Não** para desativar o Security Analytics and Logging On Prem. Pode ingerir o NetFlow no seu Coletor de fluxo. Não pode ingerir informações de eventos de firewall a partir da implementação do Firepower.
3. Selecione **OK** para confirmar a sua seleção.

   Esta é a última opção de configuração na Configuração inicial. O seu dispositivo reinicia e implementa as alterações. Depois de reiniciar, abre-se a página Login (Início de sessão).

Configuração de Nó de dados

Para Nós de dados, a Configuração inicial apresenta a seguinte configuração:

1. Configurar a porta física de gestão eth0
2. Configurar o endereço IP e a informação de gestão do dispositivo
3. Configurar eth2 e eth3 para Comunicações Inter-Nó de dados

Configurar a porta física de gestão eth0

Se configurar um Nó de dados, opcionalmente, pode configurar `eth0` como uma porta de cobre BASE-T em vez da porta SFP+ DAC predefinida. Para estes dispositivos, esta é a primeira configuração na Configuração inicial.

Antes de começar

- Se estiver a configurar um Nó de dados, consulte a folha de especificações do Secure Network Analytics relativa ao seu dispositivo para informações sobre as portas SFP+ e BASE-T suportadas.
- Se estiver a configurar um Gestor ou Coletor de fluxo compatível com Data Store, aceda a Dispositivos compatíveis com Data Store (Gestor 2210, FC 4210).
- Se estiver a configurar qualquer outro dispositivo Secure Network Analytics além de dispositivos compatíveis com Data Store, consulte Configuração geral de dispositivo Secure Network Analytics.

Procedimento

1. Inicie sessão no programa de Configuração do sistema:
   - Digite **root** e, em seguida, prima **Enter**.

     > São necessárias permissões de `root` para configurar corretamente a compatibilidade do Data Store.

   - Quando for apresentada a 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**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial e apresentada a configuração de Ordem de portas. Avance para o passo 5.

   Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.
3. A partir do menu Configuração do sistema, selecione **Rede** e, em seguida, prima **Enter**.
4. Selecione **Ordem de portas** e prima Enter.
5. Tem as seguintes opções:
   - Selecione **SFP+** para configurar o seu dispositivo para utilizar uma porta de fibra SFP+ para eth0.
   - Selecione **LOM** para configurar o seu dispositivo para utilizar uma porta de cobre BASE-T para eth0.
6. Selecione **OK** para confirmar a sua seleção.

O que fazer a seguir

- Configure o endereço IP e a informação de gestão da porta de gestão eth0. Consulte o procedimento seguinte.

Configure o endereço IP e a informação de gestão do dispositivo:

Na Configuração inicial, pode configurar o endereço IP de gestão eth0 e informação relacionada do dispositivo.

Antes de começar

- Se estiver a configurar um Nó de dados, após configurar a Ordem de portas, o assistente de Configuração inicial apresenta a configuração de gestão `eth0`. Avance para o passo 3.

Procedimento

1. Inicie sessão no programa de Configuração do sistema:
   - Se estiver a configurar um Nó de dados, digite `root` e prima **Enter**.

     São necessárias permissões de `root` para configurar corretamente o Data Store e a compatibilidade do Data Store.
   - Quando for apresentada a 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**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial.

   Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.
3. Introduza um **endereço IP** para este dispositivo.
4. Introduza a **máscara de sub-rede** da rede.
5. Introduza um endereço de **Gateway** para o endereço IP deste dispositivo.
6. Introduza um endereço de **Difusão** para o dispositivo.
7. Introduza um **Nome de anfitrião** para o seu dispositivo.
8. Introduza um **Domínio** para o seu dispositivo.

9. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

O que fazer a seguir

- Configure a informação de gestão da porta de comunicação do Nó de dados. Consulte **Configure eth2 e eth3 para Comunicações Inter-Nó de dados:** para mais informações.

Configure eth2 e eth3 para Comunicações Inter-Nó de dados:

Quando configurar um dispositivo Nó de dados, configure a porta de comunicação inter-Nó de dados com um endereço IP não encaminhável. Pode configurar uma das seguintes opções:

- `eth2`
- canal de porta com `eth2` e `eth3`

> Tem de atribuir endereços IP não encaminháveis a partir do bloco `169.254.42.0/24` CIDR .

Antes de começar

- Consulte a folha de especificações do Secure Network Analytics para o seu dispositivo para informação sobre as portas `eth2` e `eth3` SFP+ . Note que `eth2` e `eth3` dependem da forma como configura `eth0`.
- Se estiver na Configuração inicial, a Configuração do sistema apresenta a configuração de canal de porta `eth2` ou `eth2/eth3` após terminar a configuração da informação de gestão `eth0` do dispositivo. Avance para o passo 3.

Procedimento

1. A partir do menu Configuração do sistema, selecione **Rede** e, em seguida, prima **Enter**.
2. Selecione **Comunicações de nó** e prima Enter.
3. Selecione a configuração de porta de comunicação inter-Nó de dados. Tem as seguintes opções:
    - Selecione **Sim** para agregar `eth2` e `eth3` como um canal de porta para comunicações inter-Nó de dados.
    - Selecione **Não** para utilizar `eth2` para comunicações inter-Nó de dados.

4. Introduza um endereço **IP não encaminhável** a partir do bloco `169.254.42.0/24` CIDR para o canal de porta `eth2` ou `eth2/eth3`.
5. Introduza uma **Máscara de rede** de `255.255.255.0` para este endereço IP.
6. Introduza um endereço de **Gateway** para este endereço IP.
7. Introduza um endereço de **Difusão** para este endereço IP.
8. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

   Esta é a última opção de configuração na Configuração inicial. O seu dispositivo reinicia e implementa as alterações. Depois de reiniciar, abre-se a página Login (Início de sessão).

O que fazer a seguir

- Altere as palavras-passe de utilizador. Consulte **Alteração da palavra-passe do utilizador Sysadmin** para obter mais informações.

Alteração da palavra-passe do utilizador Sysadmin

Para garantir que a sua rede é segura, altere a palavra-passe predefinida para o utilizador sysadmin para os dispositivos.

Altere a palavra-passe de sysadmin:

Antes de começar

- Inicie a sessão na consola do dispositivo como **sysadmin**.
- Entre na Configuração do sistema.

Procedimento

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 cada dispositivo Secure Network Analytics é incluído na lista de anfitriões fidedignos para todos os dispositivos Secure Network Analytics 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 root**.

Alteração da palavra-passe do utilizador root

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

Altere a palavra-passe do utilizador root:

Antes de começar

- Inicie a sessão na consola do dispositivo como **sysadmin**.
- Entre na Configuração do sistema.

Procedimento

1. Aceda à shell root.
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 root.
4. Introduza a palavra-passe atual do utilizador root e, em seguida, prima **Enter**.
   É apresentada a linha de comandos da shell root.
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 root.
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 root e, em seguida, prima **Enter**.
   É apresentado um segundo pedido.
8. Volte a introduzir a palavra-passe nova do utilizador root 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 root. 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 root.
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.

Agora já está tudo a postos para configurar o seu dispositivo. Para configurar o seu dispositivo, consulte o Guia de configuração do sistema **Secure Network Analytics** relativo à sua versão de software. A Série x2xx é compatível com as versões de software 7.x do Secure Network Analytics.

Configuração do dispositivo

Agora já está tudo a postos para configurar o seu dispositivo. Para configurar o seu dispositivo, consulte o Guia de configuração do sistema **Secure Network Analytics** e o Guia de implementação e configuração do hardware do Data Store Secure Network Analytics aplicáveis à versão do seu software. A Série x2xx é compatível com as versões de software 7.x do Secure Network Analytics.

Contactar o suporte

Se precisar de suporte técnico, faça uma das seguintes ações:

- Contacte o seu Parceiro Cisco local
- Contacte o Suporte da Cisco
- Para abrir um caso na Web: http://www.cisco.com/c/en/us/support/index.html
- Para abrir um caso por e-mail: tac@cisco.com
- Para suporte por telefone: 1-800-553-2447 (EUA)
- Para números de suporte no resto do mundo: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Informação de Copyright