# Cisco Secure Network Analytics

Manual de Instalação do Dispositivo de Hardware Série x2xx 7.4.2

# Índice

# Introdução

## Descrição geral

Este guia explica como instalar os dispositivos de hardware do Cisco Secure Network Analytics (anteriormente Stealthwatch) Série x2xx. Este guia também descreve o procedimento de montagem e instalação do hardware Secure Network Analytics.

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

O hardware da Série x2xx inclui:

| **Dispositivo** | **Número de peça** |
|---|---|
| Gestor 2210<br>(anteriormente Consola de gestão Stealthwatch) | ST-SMC2210-K9 |
| Data Store 6200 (três Nós de dados) | ST-DS6200-K9 (três ST-DNODE-G1) |
| Coletor de fluxo 4210 | ST-FC4210-K9 |
| Coletor de fluxo do Motor 5210 | ST-FC5210-E |
| Coletor de fluxo da Base de dados 5210 | ST-FC5210-D |
| Encaminhador de UDP 2210 | ST-UDP2210-K9 |
| Sensor de fluxo 1210 | ST-FS1210-K9 |

| Dispositivo | Número de peça |
| --- | --- |
| Sensor de fluxo 3210 | ST-FS3210-K9 |
| Sensor de fluxo 4240 | ST-FS4240-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 já tem conhecimentos gerais acerca da instalação de equipamento de rede.

Se preferir trabalhar com um instalador profissional, contacte o seu Parceiro Cisco ou o Suporte da Cisco.

## Instalar dispositivos e configurar o sistema

Tenha em consideração o fluxo de trabalho geral de instalação e configuração do Secure Network Analytics.

1. **Instalar dispositivos:** utilize este manual de instalação para instalar os dispositivos de hardware (físicos) da Série Secure Network Analytics x2xx. Para instalar dispositivos Virtual Edition, siga as instruções no Manual de instalação dos dispositivos Virtual Edition.
2. **Configurar o Secure Network Analytics:** depois de instalar os dispositivos de hardware e virtuais, está pronto para configurar o Secure Network Analytics num sistema gerido. Siga as instruções no Guia de configuração do sistema Secure Network Analytics v7.4.2.

## Informações relacionadas

Para obter mais informações sobre o Secure Network Analytics, consulte os seguintes recursos online:

- **Informações de segurança e conformidade regulamentar:** leia o documento Informações de segurança e conformidade regulamentar antes de instalar os dispositivos da Série Secure Network Analytics x2xx.
- **Descrição geral:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Guia de design do Data Store:** https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **Matriz de suporte da versão de hardware e software:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **Especificações do dispositivo:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

## Terminologia

Este manual utiliza o termo "**dispositivo**" para qualquer produto Secure Network Analytics.

Um "**cluster**" é o grupo de dispositivos Secure Network Analytics que são geridos pelo Gestor.

## 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 |

# Sobre os dispositivos Secure Network Analytics

O 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.

## 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

Se estiver a implementar um Data Store, pode configurar um Gestor 2210 com uma interface SFP+ DAC de 10 Gbps como eth0 para maior débito. Se não estiver a implementar um Data Store, apenas pode configurar a interface de 1 Gbps/10 Gbps como eth0.

## 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.

Consulte **Secure Network Analytics com Data Store** para mais detalhes.

## 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.

Se estiver a implementar um Data Store, pode configurar um Coletor de fluxo 4210 com uma interface SFP+ DAC de 10 Gbps como eth0 para maior débito. Se não estiver a implementar um Data Store, apenas pode 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.

## 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.

Quando utilizar a configuração de elevada disponibilidade (HA) do Encaminhador de UDP, certifique-se de que liga dois dispositivos de Encaminhador de UDP através de cabos crossover. Para obter instruções, consulte **2. Ligação do dispositivo à rede**.

## 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 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:

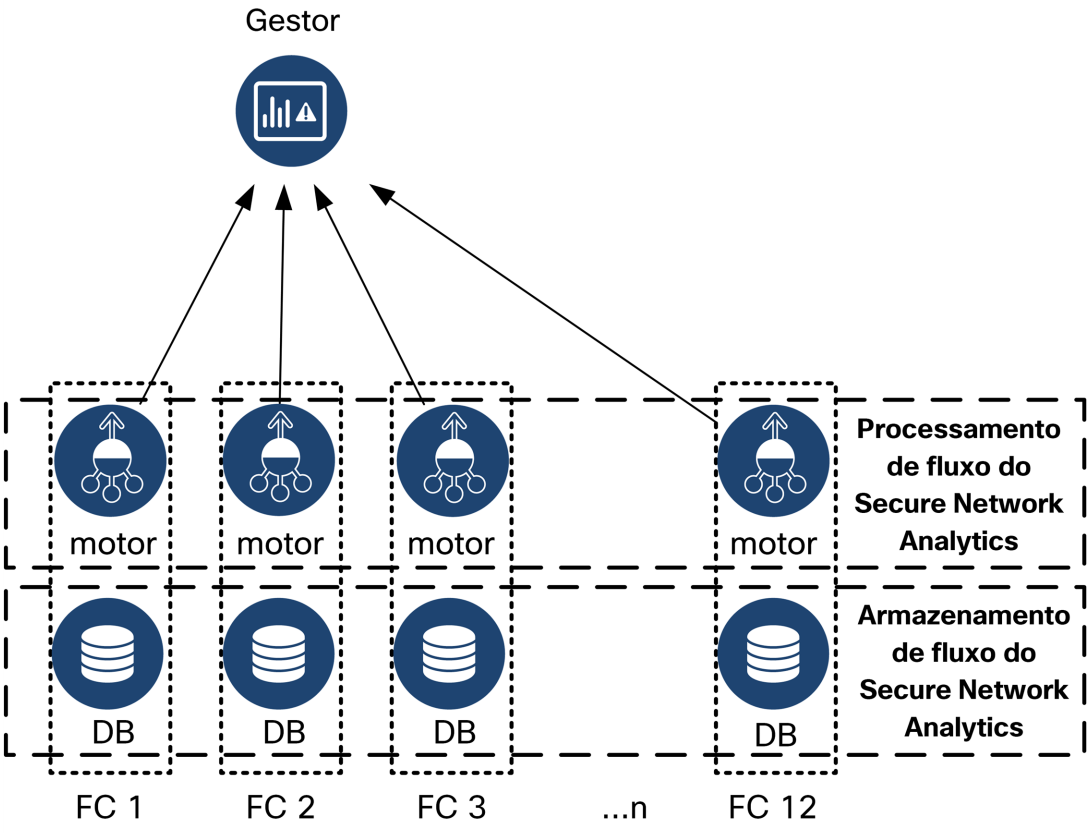
- Onde não existe NetFlow.
- Onde existe NetFlow, mas pretende obter uma maior visibilidade das métricas de desempenho e dos dados de pacote.

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.

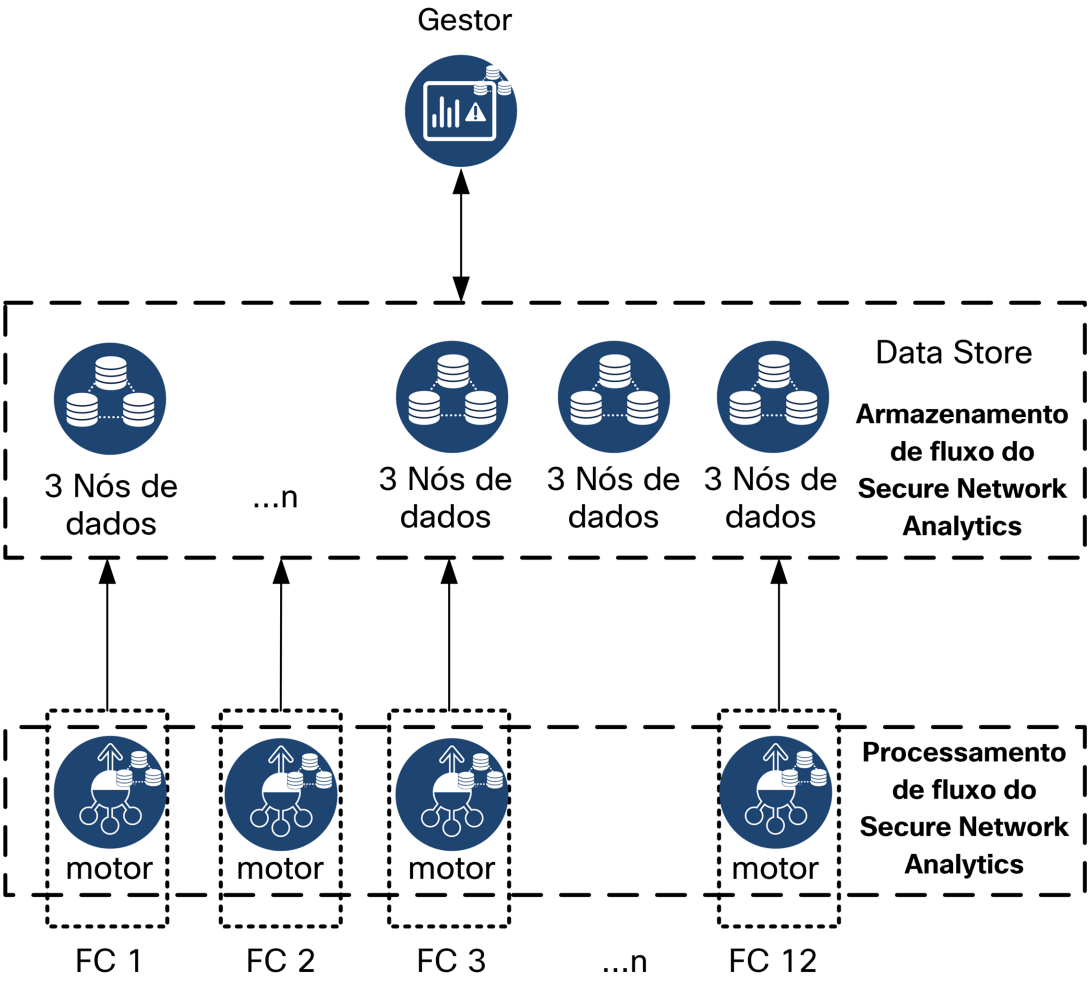
# Secure Network Analytics sem Data Store

Numa implementação do Secure Network Analytics sem um Data Store, um ou mais Coletores de fluxo ingerem e eliminam os duplicados dos dados, realizam análise e comunicam dados e resultados diretamente ao Gestor. Para resolver consultas submetidas pelo utilizador, incluindo gráficos e tabelas, o Gestor consulta todos os Coletores de fluxo geridos. Cada Coletor de fluxo devolve resultados correspondentes ao Gestor. O Gestor recolhe as informações dos diferentes conjuntos de resultados e, em seguida, gera um gráfico ou tabela que apresenta os resultados. Nesta implementação, cada Coletor de fluxo armazena dados numa base de dados local. Consulte o diagrama seguinte para obter um exemplo.



# Secure Network Analytics com Data Store

Numa implementação do Secure Network Analytics com um Data Store, o cluster do Data Store situa-se entre o seu Gestor e os Coletores de fluxo. Um ou mais Coletores de fluxo ingerem e deduplicam fluxos, realizam análise e comunicam dados e resultados diretamente ao Data Store, distribuindo-os quase equitativamente por todos os Nós de dados. O Data Store facilita o armazenamento de dados, mantém todo o seu tráfego nesse local centralizado, em vez de espalhado por vários Coletores de fluxo, e oferece uma maior capacidade de armazenamento do que múltiplos Coletores de fluxo. Consulte o diagrama seguinte para obter um exemplo.




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.

## Consultas

Para resolver consultas submetidas pelo utilizador, incluindo gráficos e tabelas, o Gestor consulta o Data Store. O Data Store localiza os resultados correspondentes nas colunas relevantes para a consulta e, em seguida, obtém as linhas correspondentes e devolve os resultados da consulta ao Gestor. O Gestor gera o gráfico ou tabela sem necessidade de recolher múltiplos conjuntos de resultados de vários Coletores de fluxo. Isto reduz o custo das consultas, em comparação com a consulta de múltiplos Coletores de fluxo, e melhora o desempenho de consulta.

## Armazenamento e tolerância a falhas do Data Store

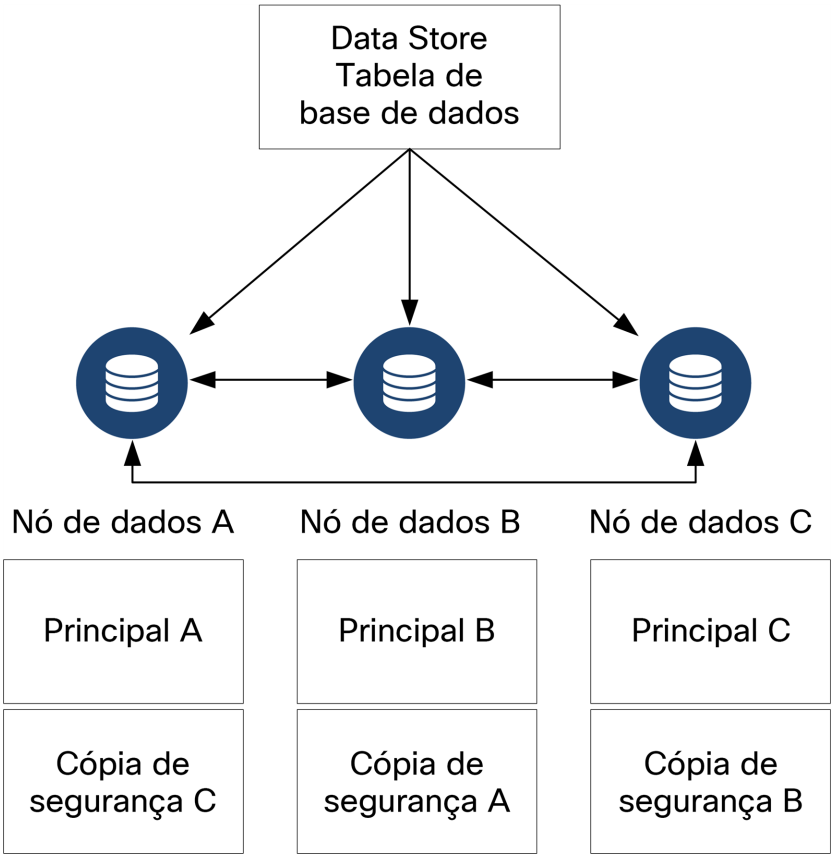
O Data Store recolhe dados de Coletores de fluxo e distribui os mesmos de forma uniforme pelos Nós de dados no cluster. Cada Nó de dados, além de armazenar uma parte da sua telemetria geral, armazena também uma cópia de segurança da telemetria de outro Nó de dados. O armazenamento de dados desta forma:

- contribui para o equilíbrio de tráfego
- distribui o processamento por cada nó
- assegura que todos os dados ingeridos no Data Store têm uma cópia de segurança para tolerância a falhas
- permite um aumento do número de Nós de dados para melhorar o desempenho geral de armazenamento e consulta

Se o Data Store tiver 3 ou mais Nós de dados e um Nó ficar inativo, desde que o Nó de dados que contém a sua cópia de segurança continue disponível e, pelo menos, metade do número total de Nós de dados continuem ativos, o Data Store geral permanece ativo. Isto dá-lhe tempo para reparar a ligação inativa ou a avaria de hardware. Após substituir o Nó de dados avariado, o Data Store restaura os dados desse nó a partir da cópia de segurança existente armazenada no Nó de dados adjacente e cria uma cópia de segurança dos dados nesse Nó de dados.

## Exemplo de armazenamento de telemetria

Consulte o diagrama seguinte para um exemplo da forma como 3 Nós de dados armazenam telemetria:



# Requisitos gerais de implementação

Antes de iniciar, consulte este guia para entender os processos, bem como a preparação, o tempo e os recursos de que precisará para planear a instalação.

## Matriz de lançamento da versão de hardware e software

Consulte os detalhes de compatibilidade na Matriz de lançamento da versão de hardware e software. A matriz está disponível em https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html.

## Especificações

Transfira a folha de especificações de cada dispositivo que planeia instalar. As especificações estão disponíveis em https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.

## Cisco Integrated Management Controller (CIMC)

Após instalar os dispositivos, certifique-se de que configura o Cisco Integrated Management Controller (CIMC) para permitir o acesso à configuração do servidor e à consola do servidor virtual. Também pode utilizar o CIMC para monitorizar o estado de funcionamento do hardware.

- **Instruções:** consulte **Ligação com CIMC (necessária para o acesso remoto)** e siga as instruções no Manual de configuração da GUI Cisco UCS C-Series Integrated Management Controller.
- **Palavra-passe predefinida:** no âmbito da configuração inicial, irá iniciar sessão no CIMC como administrador e introduzir **password** no campo Palavra-passe.
- **Requisito de palavra-passe:** depois de iniciar sessão, altere a palavra-passe predefinida para garantir a segurança da sua rede.

## Requisitos do dispositivo padrão (sem Data Store)

Se estiver a instalar o Secure Network Analytics sem um Data Store, instale os seguintes dispositivos:

| Dispositivo | Requisito |
|---|---|
| Gestor | • Mínimo de 1 Gestor |
| Coletor de fluxo | • Mínimo de 1 Coletor de fluxo |
| Sensor de fluxo | Opcional |
| Encaminhador de UDP | Opcional |

Para ver os requisitos de instalação do dispositivo para o Secure Network Analytics com um Data Store, consulte **Requisitos para a implementação do Data Store**.

## Requisitos de implementação do Gestor e Coletor de fluxo

Para cada Gestor e Coletor de fluxo que implementar, atribua um endereço IP encaminhável à porta de gestão `eth0`.

# Requisitos para a implementação do Data Store

Para implementar o Secure Network Analytics com um Data Store, consulte os requisitos e as recomendações de implementação seguintes.

## Requisitos do dispositivo (com Data Store)

A tabela seguinte fornece uma descrição geral dos dispositivos necessários para implementar o Secure Network Analytics com Data Store.

| Dispositivo | Requisito |
|---|---|
| Gestor | • Mínimo de 1 Gestor |
| Data Store | • Mínimo de 1 ou 3 Nós de dados<br>• Conjuntos adicionais de 3 Nós de dados para expandir o Data Store, máximo de 36 Nós de dados<br>• A implementação de apenas 2 Nós de dados num cluster não é suportada. |
| Coletor de fluxo | • Mínimo de 1 Coletor de fluxo |
| Encaminhador de UDP | Opcional |
| Sensor de fluxo | Opcional |

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

## Requisitos de implementação do Gestor e Coletor de fluxo

Para cada Gestor e Coletor de fluxo que implementar, atribua um endereço IP encaminhável à porta de gestão `eth0`.

- **Configuração da porta eth0:** pode configurar a utilização de uma porta 1G/10G de cobre **BASE-T** ou porta 10G de cabo twinax SFP+ para a porta de gestão `eth0` do

Gestor e Coletor de fluxo.

- **Débito:** é necessário um débito de 10G para a porta de cobre BASE-T para utilização do Data Store. Se não estiver a implementar um Data Store, apenas pode configurar a interface de cobre de 100 Mbps/1 Gbps/10 Gbps como `eth0`.

## Requisitos para a implementação do Nó de dados

Cada Data Store é composto por Nós de dados.

- **Hardware:** cada Nó de dados de hardware tem o seu próprio chassi. Quando compra um Data Store de hardware, recebe múltiplos chassis de Nó de dados de hardware, correspondentes ao número de nós indicados por esse modelo de Data Store. Por exemplo, um Data Store DS 6200 fornece 3 chassis de Nó de dados de hardware.
- **Virtual Edition:** quando transfere um Data Store virtual, pode implementar 1, 3 ou mais Nós de dados Virtual Edition (em conjuntos de 3).

> Certifique-se de que os seus Nós de dados são todos hardware ou são todos Virtual Edition. A combinação de Nós de dados virtuais e de hardware não é suportada e o hardware tem de ser da mesma geração de hardware (todos DS 6200 ou todos DN 6300).

### Implementação de vários Nós de dados

A implementação de vários Nós de dados fornece resultados de desempenho máximos. Por exemplo, um Data Store 6200 com 3 Nós de dados consegue gerir aproximadamente 1 milhão de fluxos por segundo e reter esses dados durante aproximadamente 90 dias.

Lembre-se do seguinte:

- **Conjuntos de três:** os Nós de dados podem ser agrupados em cluster como parte do seu Data Store em conjuntos de 3, entre um mínimo de 3 e um máximo de 36. A implementação de apenas 2 Nós de dados num cluster não é suportada.
- **Todos hardware ou todos virtuais:** certifique-se de que os seus Nós de dados são todos hardware ou são todos Virtual Edition. A combinação de Nós de dados de hardware e virtuais ou a combinação de Data Store 6200 e Nós de dados 6300 não é suportada.

### Implementação de um único Nó de dados

Se optar por implementar um (1) único Nó de dados:

- **Coletores de fluxo:** é suportado um máximo de 4 Coletores de fluxo.
- **Adicionar Nós de dados:** se implementar um único Nó de dados, pode adicionar Nós de dados à implementação posteriormente. Consulte os detalhes em **Implementação de vários Nós de dados**.

> Estas recomendações apenas consideram a telemetria. O seu desempenho pode variar consoante fatores adicionais, incluindo número de anfitriões, utilização de Sensor de fluxo, perfis de tráfego e outras características de rede. Contacte o Suporte da Cisco para obter ajuda com o dimensionamento.

> Atualmente, o Data Store não suporta a implementação de Nós de dados sobresselentes como substituições automáticas se um Nó de dados principal ficar inativo. Contacte o Suporte da Cisco para obter ajuda.

## Requisitos de configuração do Nó de dados

Para implementar um Data Store, atribua o seguinte a cada Nó de dados. As informações que preparar serão configuradas na Configuração inicial com o Guia de configuração do sistema.

- **Endereço IP encaminhável (eth0):** para a gestão, ingestão e comunicações de consulta com os seus dispositivos Secure Network Analytics.
- **Configuração da porta eth0:** pode configurar a utilização de uma porta 1G/10G de cobre **BASE-T** ou porta 10G de cabo twinax SFP+ para a porta de gestão `eth0`.
- **Débito:** é necessário um débito de 10G para a porta de cobre BASE-T para utilização do Data Store.
- **Comunicações inter-Nó de dados:** configure um endereço IP não encaminhável a partir do bloco CIDR `169.254.42.0/24` numa LAN ou VLAN privada para ser utilizado na comunicação inter-Nó de dados.

  Para um melhor desempenho de débito, ligue a porta `eth2` do Nó de dados (ou canal de porta com `eth2` e `eth3`) aos switches para comunicação inter-Nó de dados. Como parte do Data Store, os seus Nós de dados comunicam entre si.
- **Ligações de rede:** precisa de duas ligações de rede 10G, uma para a gestão, ingestão e comunicações de consulta e uma para comunicações inter-Nó de dados.

- **Ligação e switch adicionais:** opcionalmente, apenas em Nós de dados de hardware, para redundância de rede e criticalidade das comunicações inter-Nó de dados, instale uma ligação 10G adicional e um switch adicional para estabelecimento de um canal de porta no Nó de dados.

> Configure os seus Nós de dados de modo que os Nós de dados numerados adjacentes sejam alimentados com fontes de alimentação separadas redundantes. Esta configuração melhora a redundância dos dados e o tempo de atividade geral do Data Store.

## Considerações sobre comutação e ligação de rede

A tabela seguinte fornece uma descrição geral das considerações sobre comutação e ligação de rede quando implementa o Secure Network Analytics com um Data Store.

| Considerações sobre rede | Descrição |
|---|---|
| Comunicações inter-Nó de dados | • Estabeleça uma latência de tempo de ida e volta (RTT) recomendada inferior a 200 microssegundos entre Nós de dados.<br>• Mantenha o desfasamento de relógio em 1 segundo ou menos entre os seus Nós de dados.<br>• Estabeleça um débito recomendado de 6,4 Gbps ou superior (ligação comutada full duplex de 10 Gbps) entre os seus Nós de dados.<br>• Para Nós de dados de hardware, configurar uma porta `eth2` para um débito de 10G é suficiente para uma comunicação inter-Nó de dados normal. Criar um canal de porta acoplado `eth2/eth3` LACP para um débito até 20G permite uma comunicação mais rápida entre Nós de dados e uma adição ou substituição de Nós de dados mais rápida para o Data Store, já que cada novo Nó de dados recebe tráfego de Nós de dados adjacentes para o preenchimento dos seus dados. Tenha em atenção que a acoplagem de portas LACP é a única opção de acoplagem disponível para os Nós de dados de hardware. |

| | |
|---|---|
| Energia de Nó de dados de hardware | • Se ocorrer uma falha de energia num Nó de dados de hardware inesperadamente, os dados podem ser corrompidos. Utilize ambas as fontes de alimentação em circuitos separados de fontes de alimentação ininterruptas.<br>• Quando inicializar o cluster do Data Store, alterne a configuração do Nó de dados com base nas fontes de alimentação que cada Nó de dados utiliza. Isto permite otimizar a tolerância a falhas minimizando o número de Nós de dados que ficam inativos se ocorrer uma falha de energia. |
| Comutação de Nó de dados | • Os Nós de dados requerem a sua própria VLAN Camada 2 para permitir a comunicação inter-Nó de dados. Os Nós de dados de hardware podem ser ligados a um switch 10G partilhado ou dedicado.<br>• Recomendamos que os Nós de dados de hardware sejam ligados a 2 switches para ajudar a garantir uma conetividade constante durante as falhas e atualizações de switch. Devido à baixa latência necessária para a comunicação inter-Nó de dados, a Cisco recomenda um par redundante de switches, em que 2 switches são interligados e transportam a VLAN Camada 2 em ambos os switches. |
| Comunicações de dispositivo Secure Network Analytics | • O Gestor e os Coletores de fluxo têm de poder alcançar todos os Nós de dados<br>• Os Nós de dados têm de poder alcançar o Gestor, todos os Coletores de fluxo e cada Nó de dados |

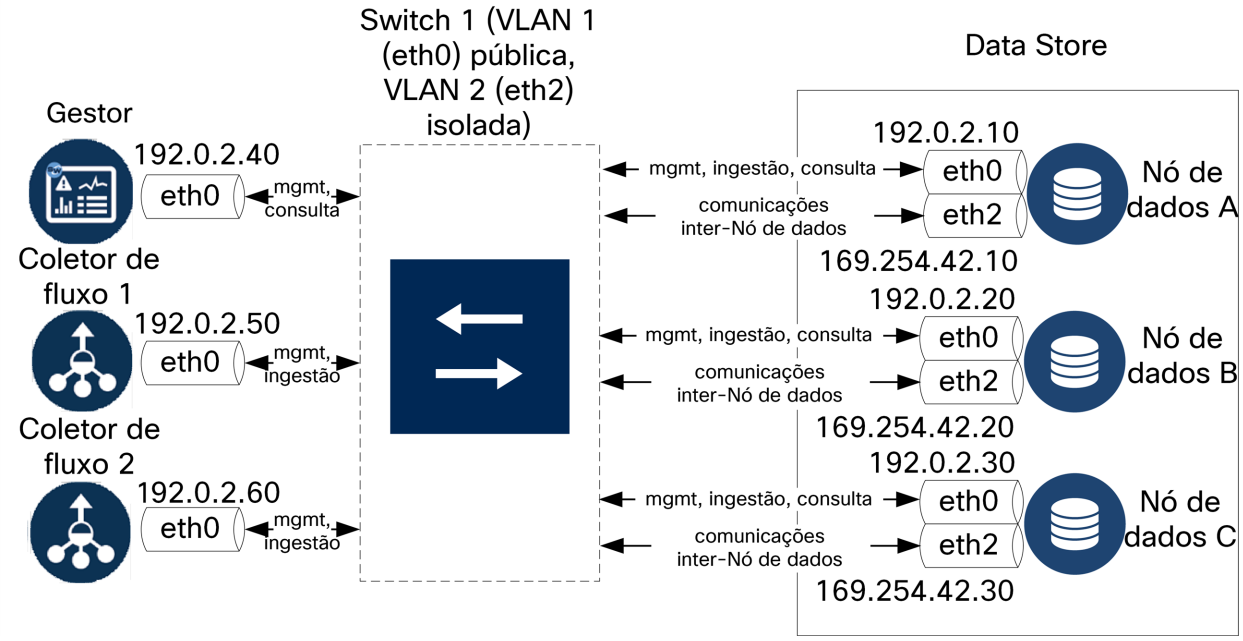
Atualmente, o Data Store não suporta a implementação de Nós de dados sobresselentes como substituições automáticas se um Nó de dados principal ficar inativo. Contacte o Suporte da Cisco para obter ajuda.

## Exemplo de comutação de hardware

Para ativar as comunicações inter-Nó de dados através de `eth2` ou do canal de porta `eth2/eth3`, implemente 1 switch que suporte velocidades de 10G.

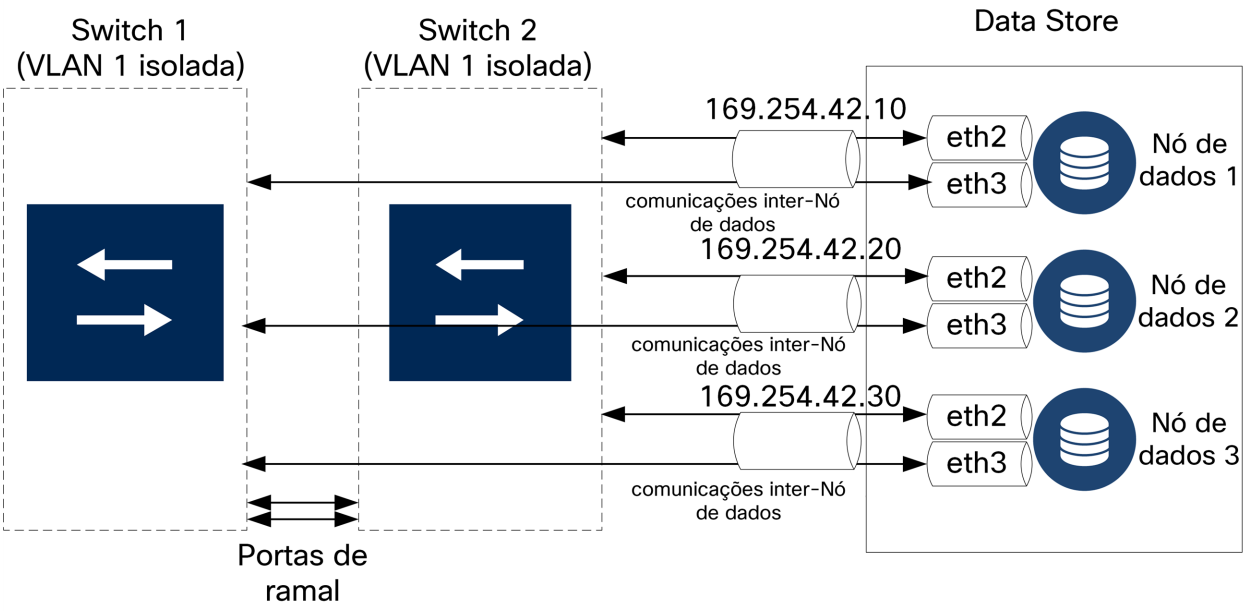
Configure uma LAN ou VLAN para comunicações de `eth0` dos Nós de dados com o Gestor e os Coletores de fluxo e uma LAN ou VLAN isolada para comunicações inter-Nó de dados.

Pode partilhar estes switches com outros dispositivos, mas deve criar LAN ou VLAN separadas para o tráfego de dispositivos adicional. Consulte o diagrama seguinte para obter um exemplo:




O cluster do Data Store requer um heartbeat contínuo entre os nós dentro da VLAN isolada. Sem este heartbeat, os Nós de dados podem, potencialmente, ficar offline, o que aumenta o risco de o Data Store ficar inativo.

Se desejar uma redundância de rede adicional, para efetuar um planeamento de acordo com as atualizações de switch e interrupções planeadas, certifique-se de que configura os seus Nós de dados com canais de porta para uma comunicação inter-Nó de dados dedicada. Ligue cada Nó de dados a 2 switches, com cada porta física ligada a um switch diferente. Consulte o diagrama seguinte para obter um exemplo:




Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento da sua implementação.

## Considerações de posicionamento do Data Store

Posicione cada Nó de dados de forma a poder comunicar com todos os seus Coletores de fluxo, o seu Gestor e os outros Nós de dados. Para um melhor desempenho, defina os seus Nós de dados e Coletores de fluxo de forma a minimizar a latência de comunicação e defina os Nós de dados e o Gestor para um desempenho de consulta ideal.

- **Firewall:** recomendamos vivamente que posicione os Nós de dados ao alcance da sua firewall, como dentro de um NOC.
- **Energia:** se o Data Store ficar inativo devido a falha de energia ou falha de hardware, correrá um risco maior de corrupção ou perda de dados. Instale os seus Nós de dados tendo em consideração um tempo de atividade constante.

Se ocorrer uma falha de energia inesperada num Nó de dados e o utilizador reiniciar o dispositivo, a instância da base de dados nesse Nó de dados pode não reiniciar automaticamente. Consulte o Guia de configuração do sistema para resolver problemas e reiniciar manualmente a base de dados.

- **Política:** certifique-se de que a política de restabelecimento de energia do Nó de dados de hardware é definida para **Restaurar o último estado**, para reiniciar o Nó de dados automaticamente após uma falha de energia e tentar restaurar os

processos em execução. Consulte o Guia de configuração da GUI UCS C-Series para mais informações sobre a configuração da política de restabelecimento de energia no CIMC.

## Requisitos de implementação do Analytics

O Secure Network Analytics utiliza a modelagem de entidades dinâmica para monitorizar o estado da sua rede. No contexto do Secure Network Analytics, uma entidade é algo que pode ser monitorizado ao longo do tempo, como um anfitrião ou um ponto final na sua rede. A modelagem de entidades dinâmica reúne informações acerca das entidades com base no tráfego que transmitem e nas atividades que executam na sua rede. Para obter mais informações, consulte Analytics: Guia de deteções, alertas e observações.

Para ativar o Analytics, a sua implementação tem de ser configurada

- numa implementação de Data Store de hardware ou virtual com qualquer número de Coletores de fluxo.
- com apenas 1 domínio de Data Store Secure Network Analytics.

# 1. Configuração da firewall para comunicações

Para as aplicações comunicarem corretamente, deve configurar a rede de forma que as firewalls ou as listas de controlo de acesso não bloqueiem as ligações necessárias. Utilize as informações fornecidas nesta secção para configurar a sua rede de forma que as aplicações possam comunicar através da rede.

## Portas abertas (todos os dispositivos)

Contacte o administrador da sua rede para garantir que as seguintes portas estão abertas e têm acesso sem restrições aos seus dispositivos (Gestors, Coletores de fluxo, Nós de dados, Sensores de fluxo e Encaminhadores de UDP):

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 8910
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

## Portas abertas adicionais para Nós de dados

Além disso, se implementar Nós de dados na sua rede, certifique-se de que as seguintes portas estão abertas e têm acesso não restrito:

- TCP 5433
- TCP 5444
- TCP 9450

## Portas e protocolos de comunicação

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

| De (Cliente) | Para (Servidor) | Porta | Protocolo |
|---|---|---|---|
| PC do Utilizador Admin | Todas as aplicações | TCP/443 | HTTPS |
| Todas as aplicações | Origem da hora da rede | UDP/123 | NTP |
| 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 |
| Encaminhador de UDP | Gestor | TCP/443 | 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 |
| Exportadores NetFlow | Coletor de fluxo (NetFlow) | UDP/2055* | NetFlow |

| De (Cliente) | Para (Servidor) | Porta | Protocolo |
|---|---|---|---|
| Exportadores sFlow | Coletor de fluxo (sFlow) | UDP/6343* | sFlow |
| Gestor | Encaminhador de UDP | TCP/443 | HTTPS |
| Gestor | Cisco ISE | TCP/443 | HTTPS |
| Gestor | Cisco ISE | TCP/8910 | XMPP |
| Gestor | DNS | UDP/53 | DNS |
| Gestor | Coletor de fluxo | TCP/443 | HTTPS |
| Gestor | Sensor de fluxo | TCP/443 | HTTPS |
| Gestor | Exportadores de fluxo | UDP/161 | SNMP |
| Gestor | LDAP | TCP/636 | TLS |
| Gestor | Pontos de distribuição de CRL | TCP/80 | HTTP |
| Gestor | Recetores do OCSP | TCP/80 | OCSP |
| PC do utilizador | Gestor | TCP/443 | HTTPS |

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

## Portas abertas adicionais para o Data Store

A secção seguinte apresenta as portas de comunicação a abrir na sua firewall para implementar o Data Store.

| # | 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 | Coletores 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 | Nó 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 |

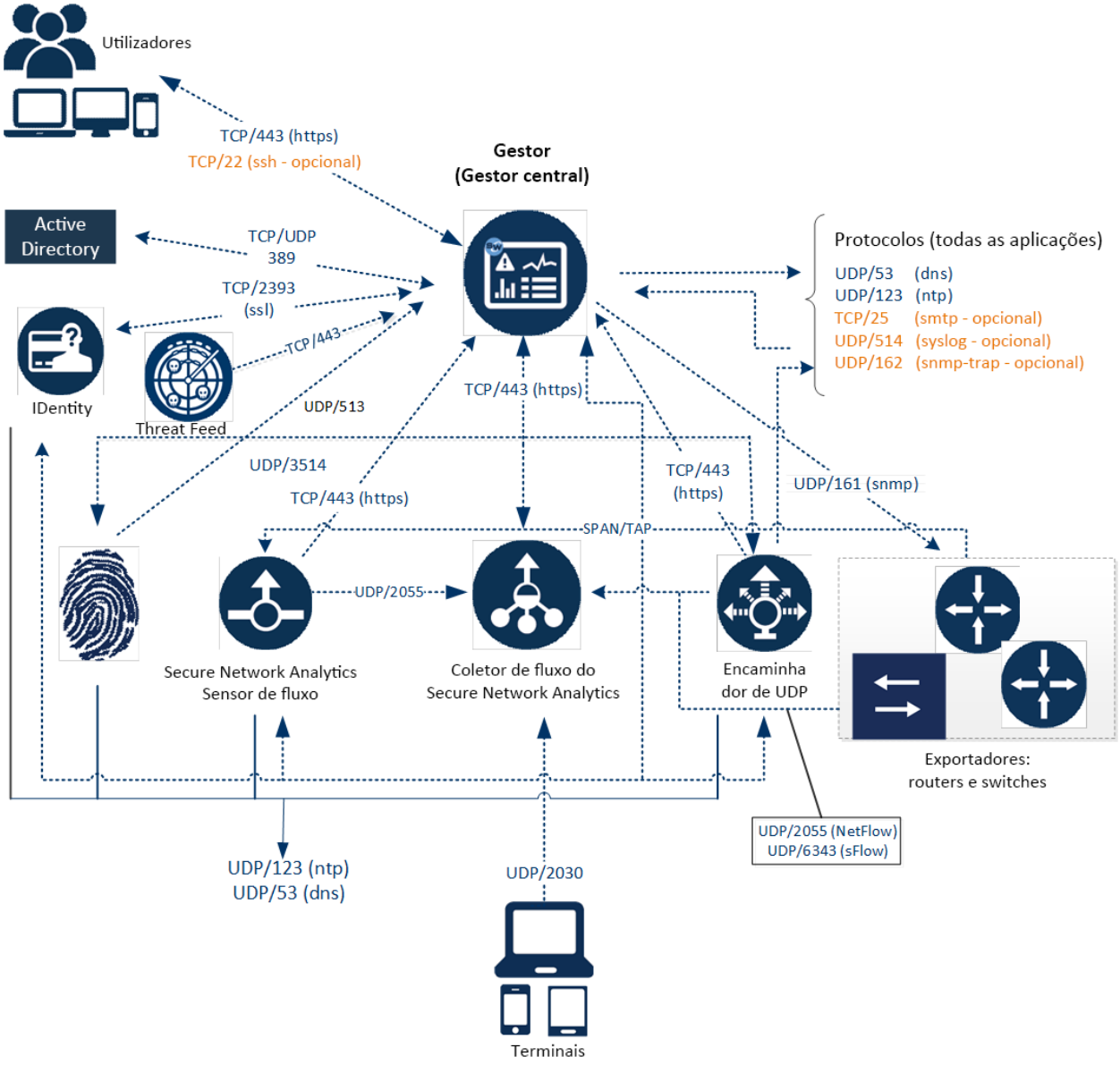
## Portas de comunicação opcionais

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

| De (Cliente) | Para (Servidor) | Porta | Protocolo |
|---|---|---|---|
| Todas as aplicações | PC do utilizador | TCP/22 | SSH |
| Gestor | Sistemas de gestão de eventos de terceiros | UDP/162 | SNMP-trap |
| Gestor | Sistemas de 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 | Todas as aplicações | TCP/22 | SSH |

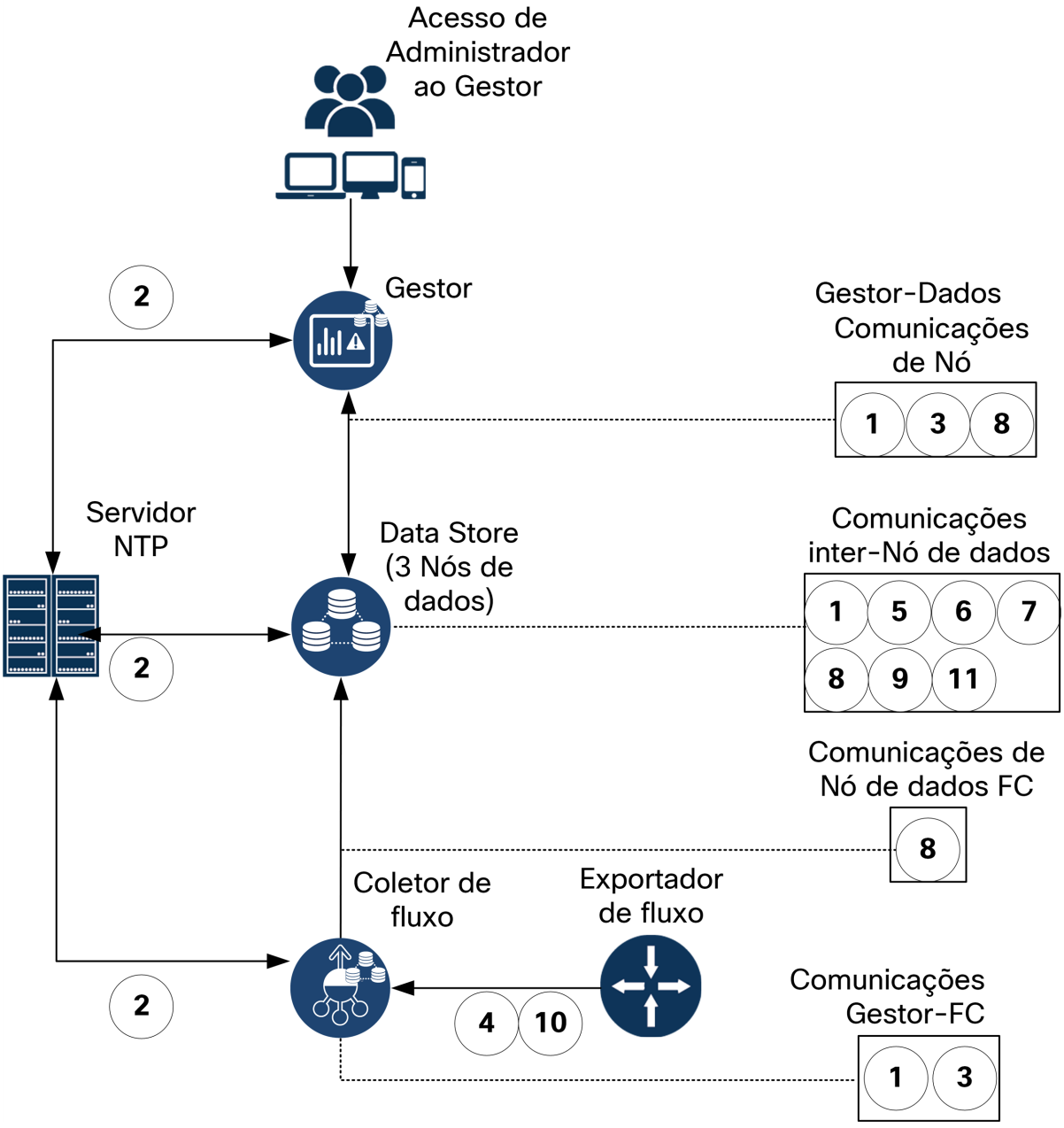
# Exemplo de implementação do Secure Network Analytics

O diagrama seguinte indica as várias ligações utilizadas pelo Secure Network Analytics. Algumas destas portas são opcionais.



# Exemplo de implementação do Secure Network Analytics com o Data Store

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.



# 2. Orientações e avisos de instalação

## Avisos de instalação

Leia o documento Informações de segurança e conformidade regulamentar antes de instalar os dispositivos da Série Secure Network Analytics 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 1004—Instruções de instalação

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

Declaração 1005—Disjuntor

Este produto confia na instalação elétrica do edifício no que respeita à proteção contra curto-circuito (sobretensão).

Declaração 1006—Aviso do chassi para montagem em rack e manutenção

Para evitar lesões corporais durante a montagem ou a manutenção desta unidade num rack, deve tomar precauções especiais para garantir que o sistema permanece estável. As orientações a seguir são fornecidas para garantir a sua segurança:

- Esta unidade deve ser montada na parte inferior do rack caso seja a única unidade no rack.
- Ao montar esta unidade num rack parcialmente cheio, carregue o rack de baixo

para cima com o componente mais pesado na parte inferior do rack.
- Ao montar esta unidade num rack parcialmente cheio, carregue o rack de baixo para cima com o componente mais pesado na parte inferior do rack.

Declaração 1015—Manuseamento da bateria

Para reduzir o risco de incêndio, explosão ou fugas de líquido inflamável ou gás:
- Substitua a bateria apenas com um tipo igual ou equivalente recomendado pelo fabricante.
- Não desmonte, esmague, fure nem utilize uma ferramenta afiada para remover, não submeta os contactos externos a curto-circuito nem elimine a bateria através de fogo.
- Não utilize se a bateria estiver amolgada ou dilatada.
- Não armazene nem utilize a bateria a uma temperatura > 60 °C.
- Não armazene nem utilize a bateria num ambiente de pressão de ar reduzida < 69,7 kPa.

Declaração 1017—Área restrita

Esta unidade destina-se a uma instalação em áreas de acesso restrito. As áreas de acesso restrito podem ser acedidas por pessoal qualificado, formado ou competente.

Declaração 191—Aviso para o Japão sobre a Classe A do Conselho de Controlo Voluntário para a Interferência (VCCI)

Este é um produto de Classe A com base na norma do Conselho VCCI. Se este equipamento for utilizado num ambiente doméstico, pode ocorrer interferência de rádio, caso em que pode ter de tomar medidas corretivas.

Declaração 164—Requisito de levantamento

São necessárias duas pessoas para erguer as secções pesadas do produto. Para evitar lesões, mantenha as costas direitas e eleve-se com as pernas, não com as costas.

Declaração 256—Aviso para a Hungria sobre a Classe A

Este equipamento é um produto de classe A e deve ser utilizado e instalado

corretamente de acordo com os requisitos húngaros de CEM da Classe A (MSZEN55022). Os equipamentos de Classe A destinam-se a estabelecimentos comerciais típicos para os quais são utilizadas condições especiais de instalação e distância de proteção.

Declaração 294—Aviso para a Coreia sobre a Classe A

Este é um dispositivo de Classe A e está registado para requisitos de compatibilidade eletromagnética (CEM) para utilização industrial. O vendedor ou o comprador devem ter conhecimento disto. Caso este tipo tenha sido vendido ou comprado por engano, deve ser substituído por um tipo para utilização residencial.

Declaração 340—Aviso sobre a Classe A para CISPR22/EN55022/CISPR32/EN55032

Este produto é de classe A. Num ambiente doméstico, este produto pode provocar interferências de radiofrequência, sendo que, nesse caso, terá de tomar medidas adequadas.

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 1028—Mais de uma fonte de alimentação

Esta unidade pode ter mais do que uma ligação de fonte de alimentação. Para reduzir o risco de choques elétricos, remova todas as ligações para desativar a unidade.

Declaração 1029—Placas frontais e painéis de cobertura

Os escudos e painéis de cobertura têm três funções importantes: reduzem o risco de choques elétricos e incêndio, contêm as interferências eletromagnéticas (EMI) que podem perturbar outros equipamentos e orientam o fluxo do ar de ventilação no interior do chassi. Não opere o sistema sem que todos os cartões, escudos, tampas frontais e tampas traseiras estejam nos devidos lugares.

Declaração 1030—Instalação do equipamento

O equipamento só deve ser instalado, substituído ou reparado por pessoas formadas e qualificadas.

Declaração 1032—Elevar o chassi

Para evitar ferimentos ou danos no chassi, nunca tente elevar ou inclinar o chassi através das pegas nos módulos, tais como fontes de alimentação, ventoinhas ou placas. Estes tipos de pegas não foram concebidos para suportar o peso da unidade.

Declaração 9001—Eliminação do produto

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

Declaração 1051—Radiação laser

As fibras e os conectores desligados podem emitir radiação laser invisível. Não olhe diretamente para feixes nem os observe diretamente com instrumentos óticos.

Declaração 1055—Laser de classe 1/1M

Radiação laser invisível presente. Não exponha a utilizadores de sistemas óticos telescópicos. Aplicável a produtos laser de Classe 1/1M.

Declaração 1008—Produto Laser Classe 1

Este produto é um produto laser de Classe 1.

Declaração 1056—Cabo de fibra sem terminais

As extremidades dos cabos de fibra ou dos conectores sem terminais podem emitir radiação laser invisível. Não observe diretamente com instrumentos óticos. A observação do laser com determinados instrumentos óticos, por exemplo, lupas e microscópios, a uma distância de 100 mm pode representar um perigo para os olhos.

| Tipo de fibra e diâmetro do núcleo (µm) | Comprimento de onda (nm) | Potência máxima (mW) | Divergência do feixe (rad) |
|---|---|---|---|
| SM 11 | 1200-1400 | 39-50 | 0,1-0,11 |
| MM 62,5 | 1200-1400 | 150 | 0,18 NA |
| MM 50 | 1200-1400 | 135 | 0,17 NA |
| SM 11 | 1400-1600 | 112-145 | 0,11-0,13 |

Declaração 1089—Definições de pessoa formada e qualificada

Entende-se por "pessoa formada" alguém que foi instruído e formado por uma pessoa qualificada e que toma as devidas precauções ao trabalhar com o equipamento.

Entende-se por "pessoa qualificada" ou competente alguém que tem formação ou experiência na tecnologia do equipamento e que entende os potenciais perigos de trabalhar com o equipamento.

Declaração 1090—Instalação por pessoa qualificada

O equipamento só deve ser instalado, substituído ou reparado por pessoas qualificadas. Consulte a declaração 1089 para obter a definição de pessoa qualificada.

Declaração 1091—Instalação por pessoa formada

O equipamento só deve ser instalado, substituído ou reparado por pessoas formadas ou qualificadas. Consulte a declaração 1089 para obter a definição de pessoa formada ou qualificada.

Declaração 1074—Cumprimento dos códigos elétricos locais e nacionais

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

Declaração 2017—Aviso sobre a Classe A para FCC

A modificação do equipamento sem autorização da Cisco pode anular a conformidade do equipamento com os requisitos FCC para dispositivos digitais de Classe A. Nesse caso, o seu direito de utilizar o equipamento pode ser limitado pelas normas FCC e pode ser-lhe solicitada a correção de quaisquer interferências em comunicações de rádio ou televisão, cujos custos ficarão a cargo do utilizador.

Este equipamento foi testado e está em conformidade com os limites para dispositivos digitais de Classe A, de acordo com a Parte 15 das Normas da FCC. Estes limites foram concebidos para garantirem proteção razoável contra interferências nocivas quando o equipamento é operado em ambientes comerciais. Este equipamento gera, utiliza e pode emitir energia de radiofrequência e, se não for instalado e utilizado de acordo com o manual de instruções, poderá provocar interferências nocivas às comunicações de rádio. O funcionamento deste equipamento numa área residencial pode provocar interferências nocivas. Neste caso, os utilizadores têm de corrigir as interferências pelos seus próprios meios.

Declaração 2021—Aviso sobre a Classe A para o Canadá

Este aparelho digital de Classe A está em conformidade com a norma ICES-003/NMB-003 do Canadá.

Declaração 7001—Mitigação de descarga eletrostática

Este equipamento pode ser sensível a descargas eletrostáticas. Utilize sempre uma pulseira antiestática no tornozelo ou no pulso antes de manusear o equipamento. Ligue a extremidade do equipamento da pulseira antiestática a uma superfície sem acabamento do chassi do equipamento ou à ficha com proteção antiestática no equipamento, se fornecida.

Declaração 7003—Requisitos de cabo blindado para picos internos do edifício provocados por trovoada

As portas intraedifício do equipamento ou subconjunto têm de utilizar cablagem intraedifício protegida que esteja ligada à terra em ambas as extremidades. As portas seguintes são consideradas portas intraedifício neste equipamento:

Declaração 7005—Picos internos do edifício provocados por trovoada e falha de alimentação AC

As portas intraedifício do equipamento ou do subconjunto apenas são adequadas para ligação a cablagem interna do edifício ou não exposta. As portas intraedifício do equipamento ou do subconjunto NÃO PODEM estar metalicamente ligadas a interfaces que, por sua vez, estejam ligadas ao fornecedor de serviços de operador (OSP) ou aos respetivos fios em mais de 6 metros. Estas interfaces destinam-se apenas a uma utilização intraedifício (portas tipo 2, 4, ou 4a, conforme descrito em GR-1089) e requerem um isolamento dos cabos do OSP expostos. A adição de protetores principais não é uma proteção suficiente para ligar estas interfaces por via metálica a um sistema de fios do OSP.
As portas seguintes são consideradas portas intraedifício no equipamento:

## 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 1075—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 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 rack aberto.
- Assegure que os racks fechados possuem uma ventilação adequada. Certifique-se de que o rack não 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.

# 3. Montar os dispositivos

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

# 4. Ligar os dispositivos 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.

## 1. Consultar as especificações

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.

- **Folhas de especificações:** para obter informações detalhadas relativas às especificações de cada dispositivo, consulte as Folhas de especificações do Secure Network Analytics.
- **Plataforma UCS:** 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.
- **Gestor 2210:** se estiver a implementar um Data Store, pode configurar um Gestor 2210 com uma interface SFP+ DAC de 10 Gbps como eth0 para maior débito. Se não estiver a implementar um Data Store, apenas pode configurar a interface de cobre de 100 Mbps/1 Gbps/10 Gbps como eth0.
- **Coletor de fluxo 4210:** se estiver a implementar um Data Store, pode configurar um Coletor de fluxo 4210 com uma interface SFP+ DAC de 10 Gbps como eth0 para maior débito. Se não estiver a implementar um Data Store, apenas pode configurar a interface de cobre de 100 Mbps/1 Gbps/10 Gbps como eth0.
- **Coletor de fluxo 5210:** o Coletor de fluxo 5210 é composto por dois servidores ligados (base de dados e motor) que funcionam 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.

  Ao configurar o seu sistema, certifique-se de que configura a base de dados e o motor pela ordem especificada no Guia de configuração do sistema.

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

## 2. Ligação do dispositivo à 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.

    - **Elevada disponibilidade do Encaminhador de UDP:** ligue os dois 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.
    - **Etiqueta Ethernet:** tome nota da etiqueta Ethernet (eth2, eth3, etc.) de cada porta. Estas etiquetas correspondem às interfaces de rede (eth2, eth3, etc.) utilizadas na configuração do sistema.

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.

# 5. Ligação do dispositivo

Esta secção descreve como ligar ao dispositivo para configuração do sistema.

Selecione o procedimento de ligação:

- **Ligação com um teclado e um monitor**
- **Ligação com cabo de série ou consola de série**
- **Ligação com CIMC (necessária para o acesso remoto)** Utilize este procedimento para ligar ao dispositivo para acesso remoto.

## 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. Ligue 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. Avance para **6. Configurar o seu Sistema Secure Network Analytics**.

## Ligação com cabo de série ou consola de série

Também pode ligar ao dispositivo com um cabo de série ou consola de série, como um computador portátil que tenha um emulador de terminal. Nas instruções, utilizamos um

computador portátil como exemplo.

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. Avance para **6. Configurar o seu Sistema Secure Network Analytics**.

## Ligação com CIMC (necessária para o acesso remoto)

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. O CIMC também será utilizado na configuração do sistema Secure Network Analytics.

1. Siga as instruções no Manual de configuração da GUI Cisco UCS C-Series Integrated Management Controller.
2. Inicie sessão no CIMC como Administrador e introduza **password** no campo Palavra-passe.
3. Altere a palavra-passe predefinida para garantir a segurança da sua rede.
4. Avance para **6. Configurar o seu Sistema Secure Network Analytics**.

# 6. Configurar o seu sistema Secure Network Analytics

Quando terminar a instalação dos seus dispositivos Virtual Edition e/ou de hardware, está pronto para configurar o Secure Network Analytics num sistema gerido.

> ⚠ Para configurar o Secure Network Analytics, siga as instruções no Guia de configuração do sistema v7.4.2. Este passo é fundamental para a configuração e a comunicação bem-sucedidas do seu sistema.
>
> Certifique-se de que configura os dispositivos pela ordem especificada no Guia de configuração do sistema.

## Requisitos de configuração do sistema

Certifique-se de que tem acesso à consola do dispositivo através do CIMC.

Utilize a tabela seguinte para preparar as informações necessárias para cada dispositivo.

| Requisito de configuração | Detalhes | Dispositivo |
|---|---|---|
| Endereço IP | Atribua um endereço IP encaminhável à porta de gestão `eth0`. | |
| Máscara de rede | | |
| Gateway | | |
| Nome do anfitrião | É necessário um nome do anfitrião único para cada aplicação. Não podemos configurar uma aplicação com o mesmo nome do anfitrião que outra aplicação. Certifique-se também de que o nome do anfitrião de cada aplicação cumpre os requisitos de padrões de Internet para anfitriões de Internet. | |

| | | |
|---|---|---|
| Nome do domínio | É necessário um nome de domínio completamente qualificado para cada aplicação. Não é possível instalar uma aplicação com um domínio vazio. | |
| Servidores DNS | Servidor DNS interno para resolução de nomes | |
| Servidores NTP | Servidor de hora interno para sincronização entre servidores. É necessário, pelo menos, 1 servidor NTP para cada dispositivo.<br>Remova o servidor NTP 130.126.24.53 se estiver na sua lista de servidores. Este servidor é conhecido como problemático e já não é suportado na nossa lista predefinida de servidores NTP. | |
| Servidor de transmissão de correio | Servidor de correio SMTP para o envio de alertas e notificações | |
| Coletor de fluxo<br>Porta de exportação | Necessária apenas para os Coletores de fluxo.<br>Predefinição NetFlow: 2055 | |
| Endereço IP não encaminhável numa LAN ou VLAN privada (para comunicação inter-Nó de dados) | Necessário apenas para Nós de dados.<br>• Eth2 de hardware ou acoplagem de eth2 e eth3. Criar um canal de porta acoplado `eth2/eth3` LACP para um débito até 20G permite uma comunicação mais rápida entre Nós de dados e uma adição ou substituição de Nós de dados mais rápida para o Data Store. Tenha em atenção que a acoplagem de portas LACP é a única opção de acoplagem disponível para os Nós de dados de | |

| | | |
|---|---|---|
| | hardware.<br>• Eth1 virtual<br><br>**Endereço IP:** pode utilizar o endereço IP fornecido ou introduzir um valor que cumpra os requisitos seguintes para as comunicações inter-Nós de dados.<br>• **Endereço IP não encaminhável** a partir do **bloco CIDR 169.254.42.0/24**, entre 169.254.42.2 e 169.254.42.254.<br>• **Três primeiros octetos:** 169.254.42<br>• **Sub-rede:** /24<br>• **Sequencial:** para que a manutenção seja mais simples, selecione endereços IP sequenciais (como 169.254.42.10, 169.254.42.11 e 169.254.42.12).<br><br>**Máscara de rede:**<br>A máscara de rede tem o código fixo 255.255.255.0 e não pode ser alterada. | |

| | | |
|---|---|---|
| Porta de ligação do hardware eth0 | Necessária apenas para dispositivos de hardware Secure Network Analytics com Data Store:<br>• Gestor 2210<br>• Coletor de fluxo 4210<br>• Nós de dados<br><br>Opções da porta de ligação do hardware eth0:<br>• **SFP+**: SFP+: porta de fibra 10G SFP+/DAC para eth0.<br>• **BASE-T**: 100 Mbs/1GbE/10GbE<br>Porta de cobre BASE-T para eth0. BASE-T é a predefinição. | |

# 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

# Histórico de alterações

| Versão do documento | Data de Publicação | Descrição |
|---|---|---|
| 1_0 | 27 de fevereiro de 2023 | Versão inicial. |
| 1_1 | 16 de março de 2023 | Foi corrigido um problema com o capítulo Requisitos gerais de implementação. |
| 1_2 | 27 de março de 2023 | Foi atualizada a tabela Portas e protocolos de comunicação. |
| 1_3 | 27 de março de 2023 | Foi corrigido um erro ortográfico. |
| 1_4 | 29 de março de 2023 | Foram adicionadas informações sobre a acoplagem de portas LACP. |
| 1_5 | 7 de junho de 2023 | Foi atualizada a secção Orientações e avisos de instalação. |