Cisco Secure Network Analytics

Guide d'installation matérielle des appliances x2xx (avec data store) 7.3.2

Sommaire

Introduction

Présentation

Ce guide explique comment installer les appliances matérielles Stealthwatch x2xx. Il décrit les composants Stealthwatch et leur placement dans le système, ainsi que l'intégration des capteurs de flux. Ce guide explique également comment monter et installer le matériel Stealthwatch. Le matériel des appliances x2xx inclut :

Appliance	**Référence**
Data store Stealthwatch 6200 (trois nœuds de données Stealthwatch)	ST-DS6200-K9 (trois ST-DNODE-G1)
Collecteur de flux Stealthwatch 4210	ST-FC4210-K9
Collecteur de flux Stealthwatch 5210 (moteur)	ST-FC5210-E
Collecteur de flux Stealthwatch 5210 (base de données)	ST-FC5210-D
Capteur de flux Stealthwatch 1210	ST-FS1210-K9
Capteur de flux Stealthwatch 3210	ST-FS3210-K9
Capteur de flux Stealthwatch 4240	ST-FS4240-K9
Console de gestion Stealthwatch 2210	ST-SMC2210-K9
Stealthwatch UDP Director 2210	ST-UDP2210-K9

Public

Ce guide est destiné au technicien chargé de l'installation du matériel Stealthwatch. Nous supposons que vous disposez déjà des connaissances générales nécessaires pour installer le matériel réseau (capteur de flux, collecteur de flux, appliance UDP Director et console de gestion Stealthwatch).

> Pour savoir comment configurer les appliances Stealthwatch, reportez-vous au **Guide de configuration du système Stealthwatch** et au Guide de déploiement et de configuration du matériel du data store Stealthwatch pour votre version logicielle. L'appliance x2xx est compatible avec les versions logicielles Stealthwatch 7.x.

Utilisation du présent guide

En plus de l'introduction, ce guide comprend les chapitres suivants :

Chapitre	Description
2 - **Points à prendre en compte pour la préconfiguration**	Les composants Stealthwatch, leur position et la configuration du pare-feu pour les communications
3 - **Préparation de l'installation**	Consignes, avertissements et recommandations relatifs à la sécurité
4- **Installation**	Montage et installation du matériel Stealthwatch

Abréviations courantes

Les abréviations suivantes apparaissent dans ce guide :

Abréviation	Description
DMZ	Zone démilitarisée (un réseau de périmètre)
HTTPS	Protocole HTTPS (Hypertext Transfer Protocol Secure)
ISE	Cisco ISE (Identity Services Engine)
Carte réseau	Carte réseau
NTP	Protocole Network Time (NTP)
PCIe	Standard Peripheral Component Interconnect Express
SNMP	Protocole SNMP (Simple Network Management Protocol)
Classes SPAN	Analyseur de port commuté
TAP	Port d'accès de test
UPS	Onduleur
VLAN	Réseau local virtuel

Points à prendre en compte pour la préconfiguration

Cette section décrit les points à prendre en compte avant d'installer et de configurer vos appliances Stealthwatch. Elle explique où placer les appliances Stealthwatch et comment les intégrer à votre réseau. Elle comprend :

Connexion avec le mot de passe par défaut du CIMC

Le contrôleur CIMC (Cisco Integrated Management Controller) permet d'accéder à la configuration du serveur, à une console de serveur virtuel et aux moniteurs surveillant l'intégrité du matériel.

- Connectez-vous au CIMC en tant qu'administrateur et saisissez **password** dans le champ Mot de passe.
- Une fois connecté, modifiez le mot de passe par défaut pour protéger la sécurité de votre réseau.

À propos des appliances Stealthwatch

Stealthwatch comporte plusieurs appliances matérielles qui recueillent, analysent et présentent des informations sur votre réseau pour améliorer ses performances et sa sécurité. Cette section décrit chaque appliance Stealthwatch x2xx.

> Pour en savoir plus, reportez-vous aux notices techniques de chaque appliance Stealthwatch x2xx.

Console de gestion Stealthwatch 2210

La console de gestion Stealthwatch gère, coordonne, configure et organise les différents composants du système. Le logiciel Stealthwatch vous permet d'accéder à l'interface utilisateur web de la console depuis un ordinateur muni d'un navigateur web. Vous pouvez facilement accéder en temps réel aux informations de sécurité et de réseau concernant les segments essentiels de votre entreprise. Indépendante de toute plateforme grâce à Java, la console de gestion Stealthwatch permet ce qui suit :

- Gestion, configuration et création de rapports centralisées pour 25 collecteurs de flux Stealthwatch
- Création de graphiques pour visualiser le trafic
- Analyse approfondie pour le dépannage
- Rapports consolidés et personnalisables
- Analyse des tendances
- Surveillance des performances
- Notification immédiate des failles de sécurité

Les utilisateurs qui déploient un data store peuvent configurer une console de gestion Stealthwatch 2210 avec une interface DAC SFP+ 10 Gbit/s sur eth0 pour un débit accru. Les utilisateurs qui ne déploient pas de data store peuvent uniquement configurer l'interface cuivre 100 Mbit/s, 1 Gbit/s, 10 Gbit/s sur eth0.

Collecteurs de flux Stealthwatch 4210 et 5210

Le collecteur de flux Stealthwatch collecte des données NetFlow, cFlow, J-Flow, Packeteer 2, NetStream et IPFIX pour assurer la protection du réseau basée sur le comportement.

Le collecteur de flux regroupe les données sur les comportements de plusieurs réseaux ou segments de réseau haut débit pour garantir une protection complète et améliorer les performances sur l'ensemble des réseaux répartis dans différentes zones géographiques.

Les utilisateurs qui déploient un data store peuvent configurer un collecteur de flux 4210 avec une interface DAC SFP+ 10 Gbit/s sur eth0 pour un débit accru. Les utilisateurs qui ne déploient pas de data store peuvent uniquement configurer l'interface cuivre 100 Mbit/s, 1 Gbit/s, 10 Gbit/s sur eth0.

> À partir des données qu'il reçoit, le collecteur de flux identifie les attaques connues ou inconnues, les utilisations frauduleuses internes et les périphériques réseau mal configurés, quel que soit le chiffrement ou la fragmentation des paquets. Dès que Stealthwatch identifie un comportement suspect, le système exécute l'action que vous avez configurée, le cas échéant, pour ce type de comportement.

Data store Stealthwatch 6200

Le data store Stealthwatch fournit un référentiel central pour stocker les données de télémétrie de votre réseau récoltées par vos collecteurs de flux Stealthwatch. Le data store se compose d'un cluster de nœuds de données, contenant chacun une partie de

vos données, ainsi qu'une sauvegarde des données d'un nœud de données distinct. Comme toutes vos données se trouvent dans une base de données centralisée au lieu d'être réparties sur plusieurs collecteurs de flux, votre console de gestion Stealthwatch peut récupérer les résultats de la requête auprès du data store plus rapidement que si elle interrogeait tous vos collecteurs de flux séparément. Le cluster du data store offre une meilleure tolérance aux pannes, une réponse améliorée aux requêtes et un remplissage plus rapide des graphiques.

Capteurs de flux Stealthwatch 1210, 3210 et 4240

Le capteur de flux Stealthwatch est une appliance réseau qui fonctionne de la même manière qu'une appliance de capture de paquets classique ou qu'un IDS du fait qu'il se branche à un port SPAN (switch port analyzer), à un port miroir ou à un port TAP Ethernet. Le capteur de flux augmente la visibilité sur les zones de réseau suivantes :

- Où NetFlow n'est pas disponible.
- Où NetFlow est disponible, mais vous voulez une meilleure visibilité sur les indicateurs de performance et les données des paquets.

En orientant le capteur de flux vers un collecteur de flux NetFlow v9, vous pouvez obtenir des statistiques détaillées et utiles sur le trafic à partir de ce collecteur. Associé au collecteur de flux Stealthwatch, le capteur de flux fournit également des informations détaillées sur les indicateurs de performance et de comportement. Les indicateurs de performance, quant à eux, donnent des informations sur la latence aller-retour introduite par le réseau ou par l'application côté serveur.

Étant donné que le capteur de flux bénéficie d'une visibilité sur les paquets, il peut calculer le délai de retransmission (RTT), le délai de réponse du serveur (SRT) et la perte de paquets pour les sessions TCP. Il inclut tous les champs supplémentaires dans les enregistrements NetFlow qu'il envoie au collecteur de flux.

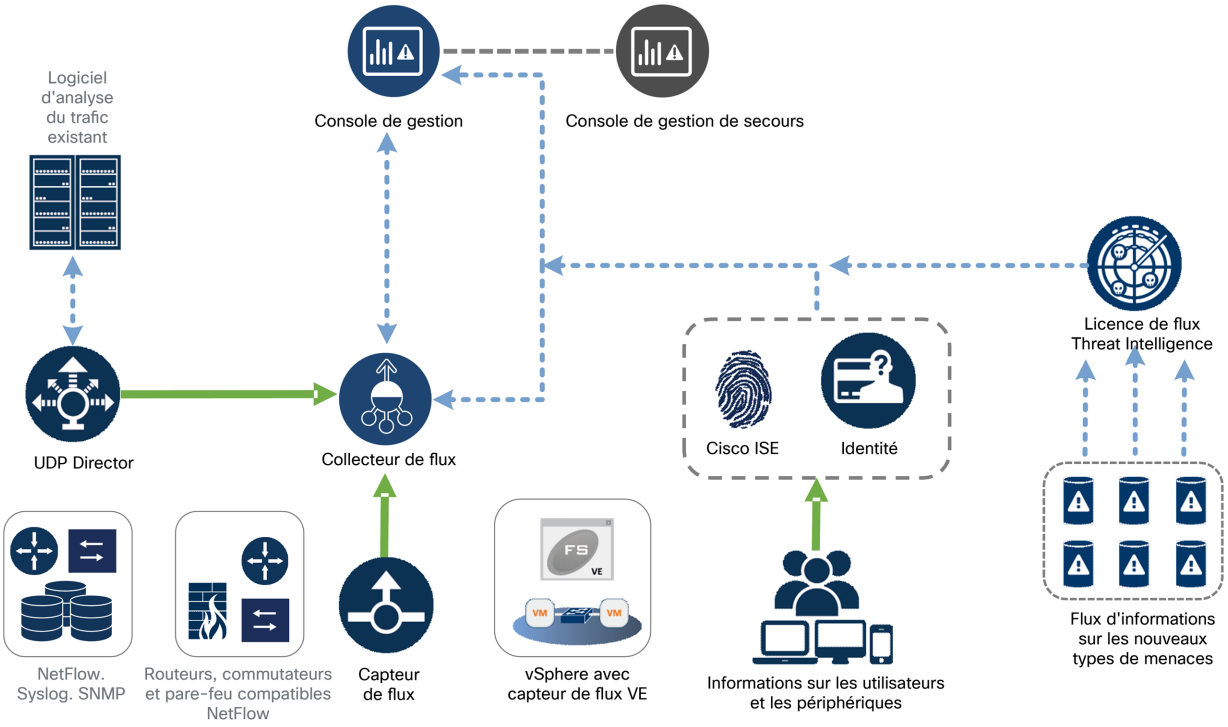
Stealthwatch UDP Director 2210

L'appliance Stealthwatch UDP Director est un réplicateur de paquets UDP haut débit ultraperformant. L'appliance UDP Director est très utile, car elle envoie les déroutements NetFlow, sFlow, syslog ou SNMP (Simple Network Management Protocol) à divers collecteurs. Elle reçoit des données des applications UDP hors connexion, puis les retransmet à plusieurs destinataires en dupliquant les données le cas échéant.

Lorsque vous utilisez la configuration UDP Director haute disponibilité (HA) (basculement), vous devez connecter deux appliances UDP Director avec des câbles croisés. Pour obtenir des instructions spécifiques, reportez-vous à **Connexion de votre appliance au réseau**.

Placement des appliances

Comme le montre la figure ci-dessous, vous pouvez déployer stratégiquement des appliances Stealthwatch pour assurer une couverture optimale des segments clés du réseau, dans le réseau interne, au niveau du périmètre ou dans la DMZ.



Placement de la console de gestion Stealthwatch

Étant donné qu'il s'agit d'un périphérique de gestion, installez la console de gestion Stealthwatch à un emplacement de votre réseau accessible à tous les périphériques qui lui envoient des données.

Si vous disposez de deux consoles de gestion Stealthwatch à des fins de basculement, nous vous recommandons d'installer les consoles principale et secondaire dans des emplacements physiques distincts. Cette stratégie améliore la reprise après sinistre si nécessaire.

Placement du collecteur de flux Stealthwatch

En tant que périphérique de collecte et de surveillance, le collecteur de flux Stealthwatch doit être installé à un emplacement de votre réseau accessible aux périphériques NetFlow ou sFlow qui lui envoient des données, ainsi qu'aux périphériques que vous envisagez d'utiliser pour accéder à l'interface de gestion.

Lorsque vous placez un collecteur de flux en dehors d'un pare-feu, nous vous recommandons de désactiver le paramètre **Accept traffic from any exporter** (Accepter le trafic de chaque exportateur).

Placement du capteur de flux Stealthwatch

Le capteur de flux Stealthwatch, qui est un périphérique de surveillance passif, peut être placé à différents points sur votre réseau pour observer et enregistrer l'activité IP. Ainsi, il détecte les failles de sécurité pour assurer l'intégrité du réseau. Les fonctionnalités de capteur de flux intègrent des systèmes de gestion web qui facilitent l'administration et la gestion centralisées ou à distance.

L'appliance de capteur de flux est plus efficace lorsqu'elle est placée au niveau de segments critiques de votre réseau d'entreprise comme suit :

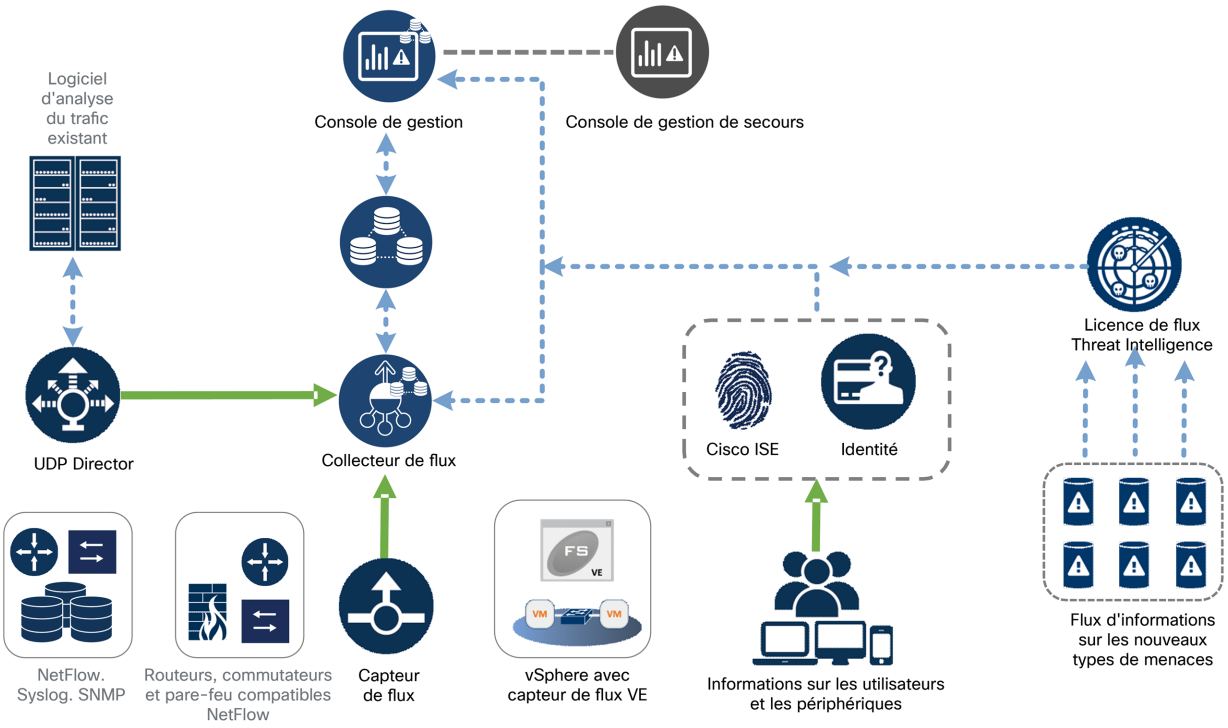
- À l'intérieur du pare-feu pour surveiller le trafic et déterminer si une faille de pare-feu s'est produite.
- En dehors de votre pare-feu pour surveiller les flux de trafic et déterminer ce qui menace votre pare-feu.
- Au niveau des segments stratégiques de votre réseau pour le protéger contre les collaborateurs mécontents ou les hackers avec des droits d'accès d'utilisateur root.
- Dans des bureaux distants qui constituent des extensions de réseau vulnérables.
- Sur votre réseau d'entreprise à des fins de gestion d'utilisation des protocoles (par exemple, sur votre sous-réseau de services de transaction pour déterminer si un hacker a recours au protocole Telnet ou FTP pour compromettre les données financières de vos clients).

Placement de Stealthwatch UDP Director

La seule condition à prendre en compte pour le placement de l'appliance Stealthwatch UDP Director est de veiller à ce qu'aucun obstacle ne l'empêche de communiquer avec vos autres appliances Stealthwatch.

> ⚠ Si vous déployez UDP Director dans un environnement dans lequel Cisco ACI est utilisé et où la fonction uRPF (Unicast Reverse Path Forwarding) ou d'**apprentissage IP limité au sous-réseau** est activée, le réseau local peut bloquer le trafic transféré quittant UDP Director. Vous devez usurper le trafic UDP dans le cadre des règles de transfert afin que les outils collectant les données du journal puissent connaître la source du trafic.
>
> Pour garantir le bon fonctionnement de UDP Director dans ce cas, déployez votre appliance UDP Director sur une partie du réseau dans laquelle vous pouvez désactiver le protocole uRPF ou **limiter l'apprentissage IP au sous-réseau** (généralement en interne). Vous pouvez placer UDP Director dans une sortie L3 (aucun apprentissage IP). Si vous utilisez la version 4.0+, vous pouvez désactiver la détection des terminaux sur chaque VRF individuellement.

Le schéma suivant illustre un déploiement Stealthwatch avec un data store.

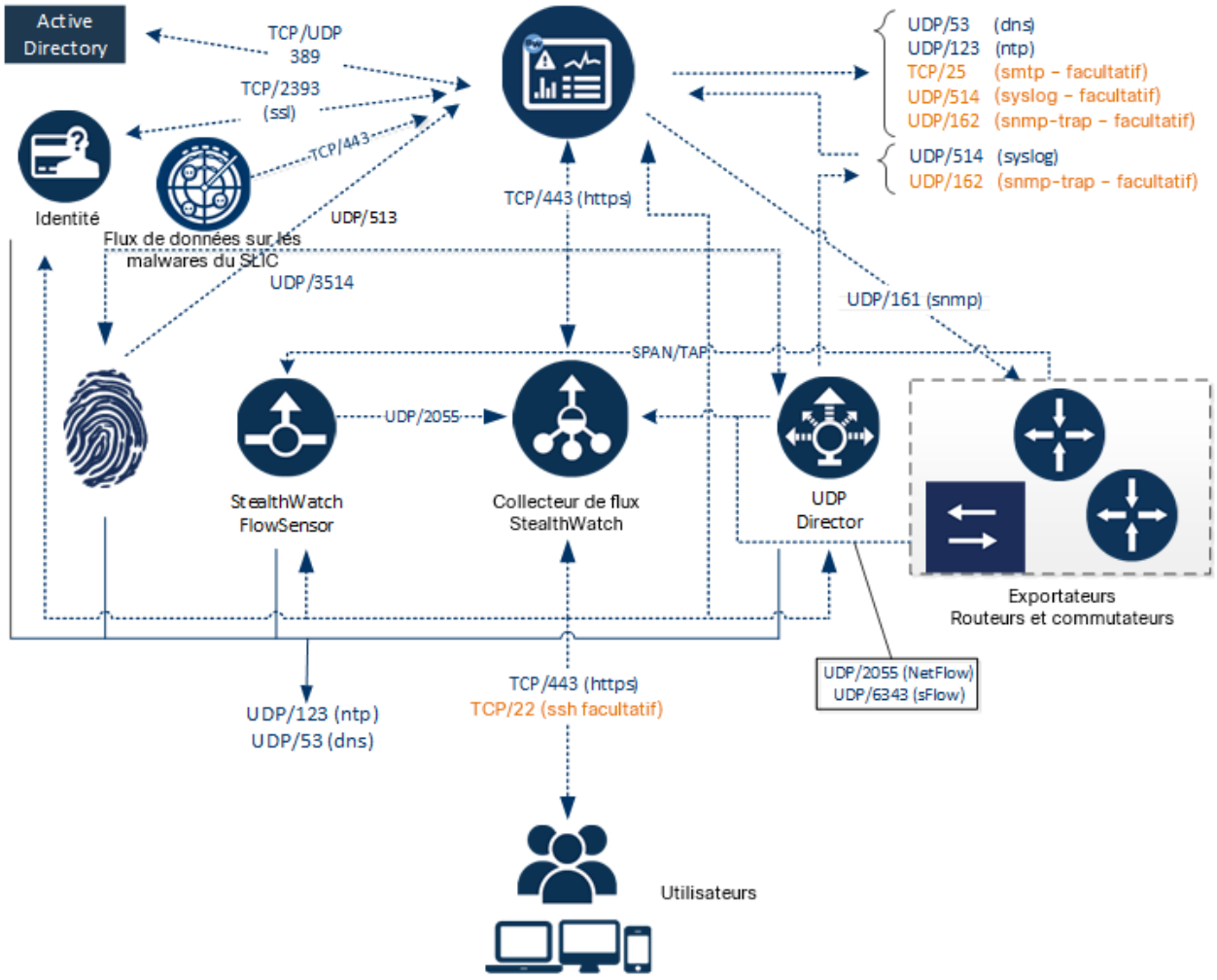


Placement du data store Stealthwatch

En tant que référentiel pour les données récoltées par les collecteurs de flux et en tant que référentiel centralisé sur lequel une console de gestion Stealthwatch exécute des requêtes, installez vos nœuds de données à un emplacement du réseau accessible par tous vos collecteurs de flux et votre console de gestion Stealthwatch. Consultez le Guide de déploiement et de configuration du matériel du data store pour en savoir plus.

Ports de communication

Le schéma suivant présente les ports de communication à ouvrir dans votre déploiement Stealthwatch.



Le tableau suivant montre comment les ports sont utilisés dans Stealthwatch :

De (client)	À (serveur)	Port	Protocole
Ordinateur de l'utilisateur admin	Tous les appareils	TCP/443	HTTPS
Tous les appareils	Source d'heure réseau	UDP/123	NTP
Active Directory	Console de gestion Stealthwatch	TCP/389, UDP/389	LDAP

De (client)	À (serveur)	Port	Protocole
Cisco ISE	Console de gestion Stealthwatch	TCP/443	HTTPS
Cisco ISE	Console de gestion Stealthwatch	TCP/5222	XMPP
Sources de journalisation externes	Console de gestion Stealthwatch	UDP/514	SYSLOG
Collecteur de flux	Console de gestion Stealthwatch	TCP/443	HTTPS
SLIC	Console de gestion Stealthwatch	TCP/443 ou connexion avec proxy	HTTPS
UDP Director	Collecteur de flux – sFlow	UDP/6343	sFlow
UDP Director	Collecteur de flux – NetFlow	UDP/2055*	NetFlow
UDP Director	Systèmes de gestion d'événements tiers	UDP/514	SYSLOG
Capteur de flux	Console de gestion Stealthwatch	TCP/443	HTTPS
Capteur de flux	Collecteur de flux – NetFlow	UDP/2055	NetFlow
Identité	Console de gestion Stealthwatch	TCP/2393	SSL
Exportateurs NetFlow	Collecteur de flux – NetFlow	UDP/2055*	NetFlow
Exportateurs sFlow	Collecteur de flux – sFlow	UDP/6343*	sFlow
Console de gestion Stealthwatch	Cisco ISE	TCP/443	HTTPS

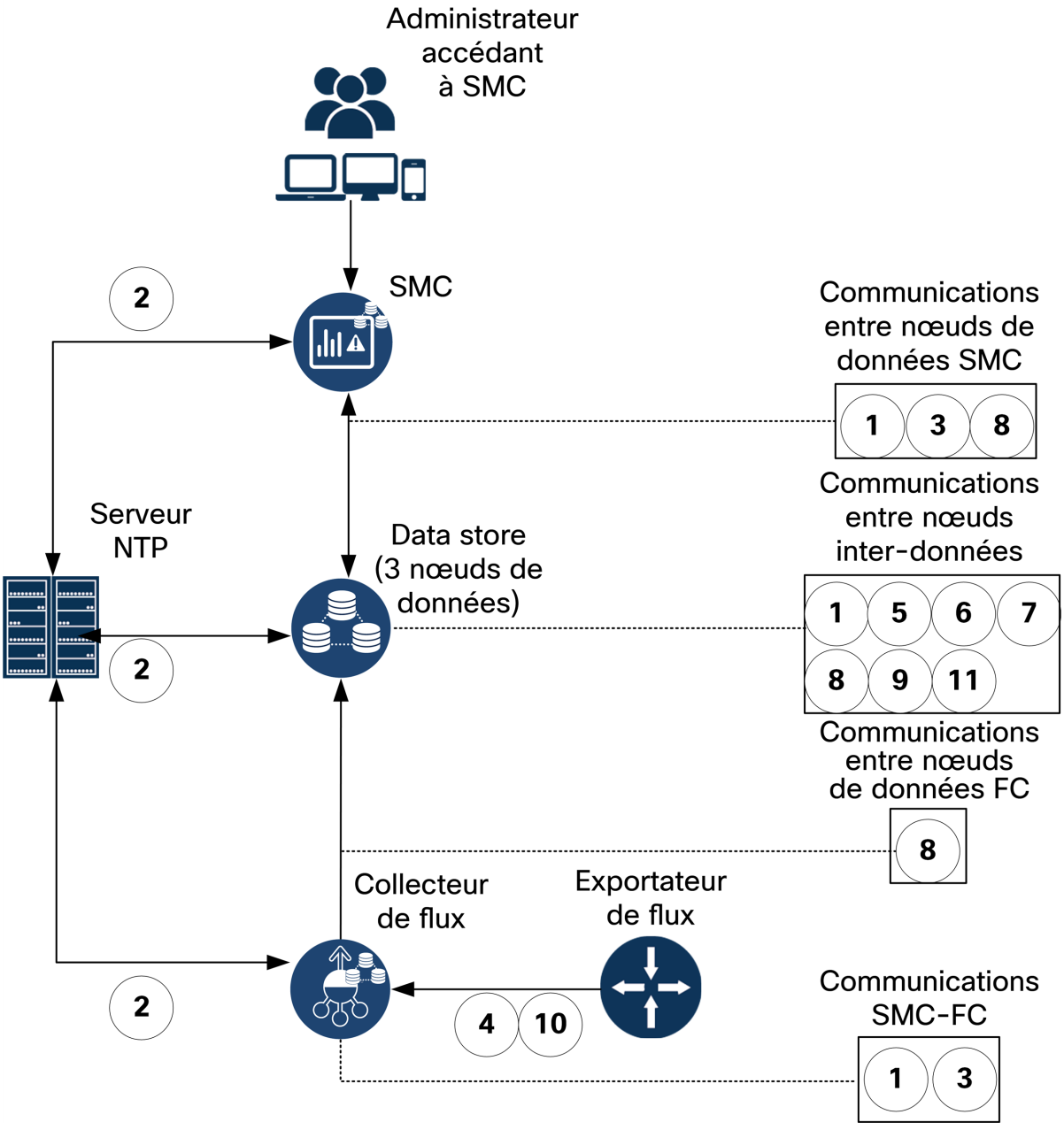
De (client)	À (serveur)	Port	Protocole
Console de gestion Stealthwatch	DNS	UDP/53	DNS
Console de gestion Stealthwatch	Collecteur de flux	TCP/443	HTTPS
Console de gestion Stealthwatch	Capteur de flux	TCP/443	HTTPS
Console de gestion Stealthwatch	Identité	TCP/2393	SSL
Console de gestion Stealthwatch	Exportateurs de flux	UDP/161	SNMP
PC utilisateur	Console de gestion Stealthwatch	TCP/443	HTTPS

*C'est le port par défaut, mais tout port UDP peut être configuré sur l'exportateur.

Le tableau suivant concerne les configurations facultatives en fonction des exigences d'administration de votre réseau :

De (client)	À (serveur)	Port	Protocole
Tous les appareils	PC utilisateur	TCP/22	SSH
Console de gestion Stealthwatch	Gestion d'événements tiers	UDP/162	SNMP-trap
Console de gestion Stealthwatch	Gestion d'événements tiers	UDP/514	SYSLOG
Console de gestion Stealthwatch	Passerelle de messagerie	TCP/25	SMTP
Console de gestion Stealthwatch	SLIC	TCP/443	SSL
PC utilisateur	Tous les appareils	TCP/22	SSH

Le schéma suivant présente les ports supplémentaires à ouvrir si vous déployez un data store sur votre réseau :



Le tableau suivant présente les ports utilisés si vous déployez un data store sur votre réseau :

N°	**De (client)**	**À (serveur)**	**Port**	**Protocole ou objectif**
1	SMC	Collecteurs de flux et nœuds de données	22/TCP	SSH, requis pour initialiser la base de données du data store
1	Nœuds de données	Tous les autres nœuds de données	22/TCP	SSH, requis pour initialiser la base de données du data store et pour exécuter les tâches d'administration de la base de données
2	SMC, collecteurs de flux et nœuds de données	Serveur NTP	123/UDP	NTP, requis pour la synchronisation de l'heure
2	Serveur NTP	SMC, collecteurs de flux et nœuds de données	123/UDP	NTP, requis pour la synchronisation de l'heure
3	SMC	Collecteurs de flux et nœuds de données	443/TCP	HTTPS, requis pour sécuriser les communications entre les appliances
3	Collecteurs de flux	SMC	443/TCP	HTTPS, requis pour sécuriser les communications entre les appliances
3	Nœuds de données	SMC	443/TCP	HTTPS, requis pour sécuriser les communications entre les appliances

4	Exportateurs NetFlow	Collecteurs de flux – NetFlow	2055/UDP	Intégration NetFlow
5	Nœuds de données	Tous les autres nœuds de données	4803/TCP	Service de messagerie inter-nœuds de données
6	Nœuds de données	Tous les autres nœuds de données	4803/UDP	Service de messagerie inter-nœuds de données
7	Nœuds de données	Tous les autres nœuds de données	4804/UDP	Service de messagerie inter-nœuds de données
8	SMC, collecteurs de flux et nœuds de données	Nœuds de données	5433/TCP	Connexions client Vertica
9	Nœud de données	Tous les autres nœuds de données	5433/UDP	Surveillance du service de messagerie Vertica
10	Exportateurs sFlow	Collecteur de flux – sFlow	6343/UDP	Intégration sFlow
11	Nœuds de données	Tous les autres nœuds de données	6543/UDP	Service de messagerie inter-nœuds de données

Intégration du capteur de flux dans votre réseau

Polyvalent, le capteur de flux Stealthwatch s'intègre avec une grande variété de topologies, technologies et composants de réseau. Même si toutes les configurations ne peuvent pas être traitées ici, les exemples pourront vous aider à déterminer la meilleure configuration pour vos besoins.

Avant d'installer un capteur de flux, vous devez prendre plusieurs décisions concernant votre réseau et comment vous souhaitez le surveiller. Par conséquent, veillez à bien analyser la topologie de votre réseau et vos besoins de surveillance. Nous vous recommandons de connecter un capteur de flux afin qu'il reçoive les transmissions vers et depuis le réseau surveillé et, si besoin, également les transmissions de réseau interne.

Les sections suivantes expliquent comment intégrer une appliance de capteur de flux Stealthwatch dans votre réseau à l'aide des périphériques réseau Ethernet suivants :

- **Ports TAP**
- **Ports SPAN**

Ports TAP

Lorsqu'un port d'accès de test (TAP) est placé dans le cadre d'une connexion réseau, il répète la connexion sur un ou plusieurs ports distincts. Par exemple, un port TAP Ethernet connecté avec un câble Ethernet répétera chaque direction de transmission sur plusieurs ports distincts. Par conséquent, l'utilisation d'un port TAP est la façon la plus fiable d'utiliser le capteur de flux. Le type de port TAP que vous utilisez dépend de votre réseau.

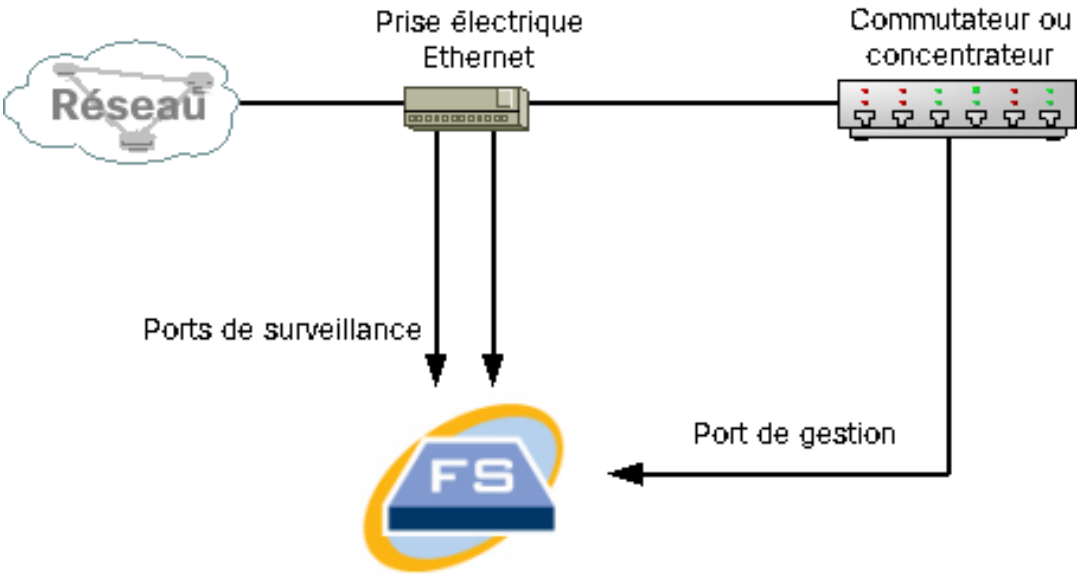
Cette section explique les différentes manières d'utiliser des ports TAP :

- **Utilisation de ports TAP électriques**
- **Utilisation de ports TAP optiques**
- **Utilisation de ports TAP hors de votre pare-feu**
- **Placement du capteur de flux à l'intérieur du pare-feu**

Dans un réseau utilisant des ports TAP, le capteur de flux capture des données de surveillance des performances uniquement s'il est connecté à un port TAP de regroupement surveillant à la fois le trafic entrant et sortant. Si le capteur de flux est connecté à un port TAP unidirectionnel qui capture uniquement une direction du trafic sur chaque port, le capteur de flux ne capture pas les données de surveillance des performances.

Utilisation de ports TAP électriques

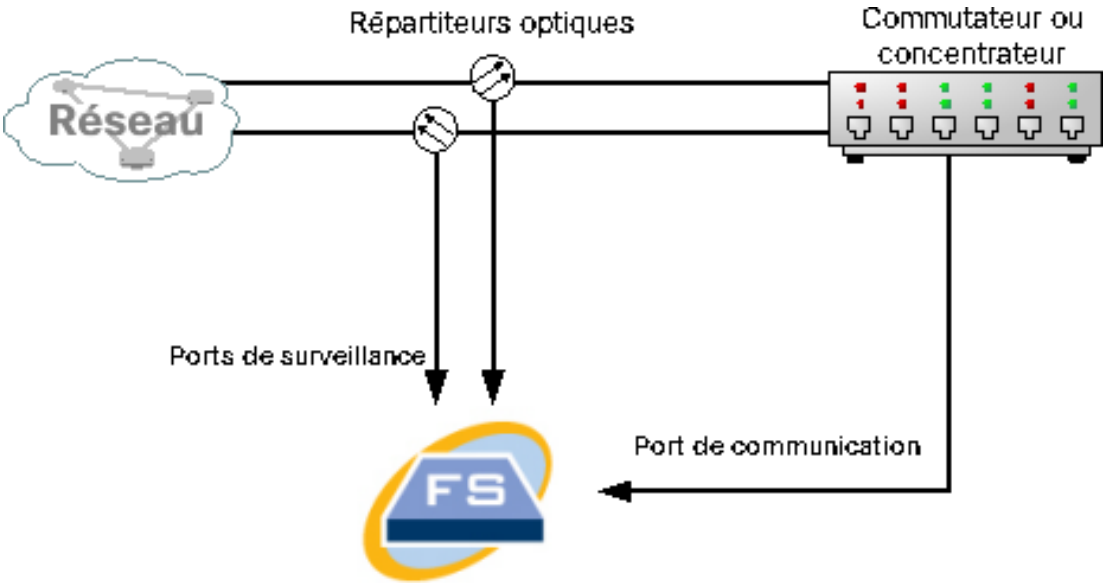
Dans l'exemple ci-dessous, le capteur de flux est connecté à un port TAP Ethernet électrique. Pour ce faire, connectez les deux ports TAP aux ports 1 et 2 du moniteur du capteur de flux.



Utilisation de ports TAP optiques

Utilisez deux répartiteurs pour les systèmes à fibre optique. Placez un répartiteur de câble à fibre optique dans chaque direction de transmission pour répéter le signal optique pour une seule direction de transmission.

Dans l'exemple ci-dessous, le capteur de flux est connecté à un réseau à fibre optique. Pour ce faire, connectez les sorties des répartiteurs aux ports 1 et 2 du moniteur du capteur de flux.



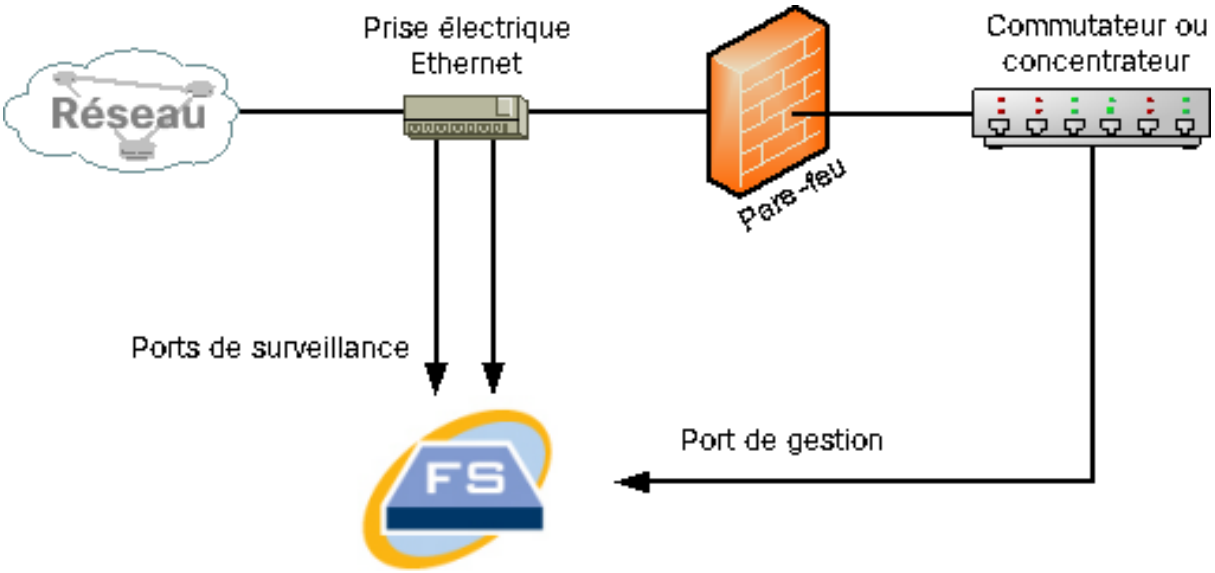
Si la connexion entre les réseaux surveillés est une connexion optique, alors le capteur de flux est connecté à deux répartiteurs optiques. Le port de gestion est connecté soit au commutateur du réseau surveillé, soit à un autre commutateur ou à un concentrateur.

Utilisation de ports TAP hors de votre pare-feu

Pour que le capteur de flux surveille le trafic entre votre pare-feu et d'autres réseaux, connectez le port de gestion Stealthwatch à un commutateur ou à un port à l'extérieur du pare-feu.

Nous vous recommandons vivement d'utiliser un port TAP pour cette connexion afin d'éviter qu'une panne du périphérique ne bloque le fonctionnement de votre réseau.

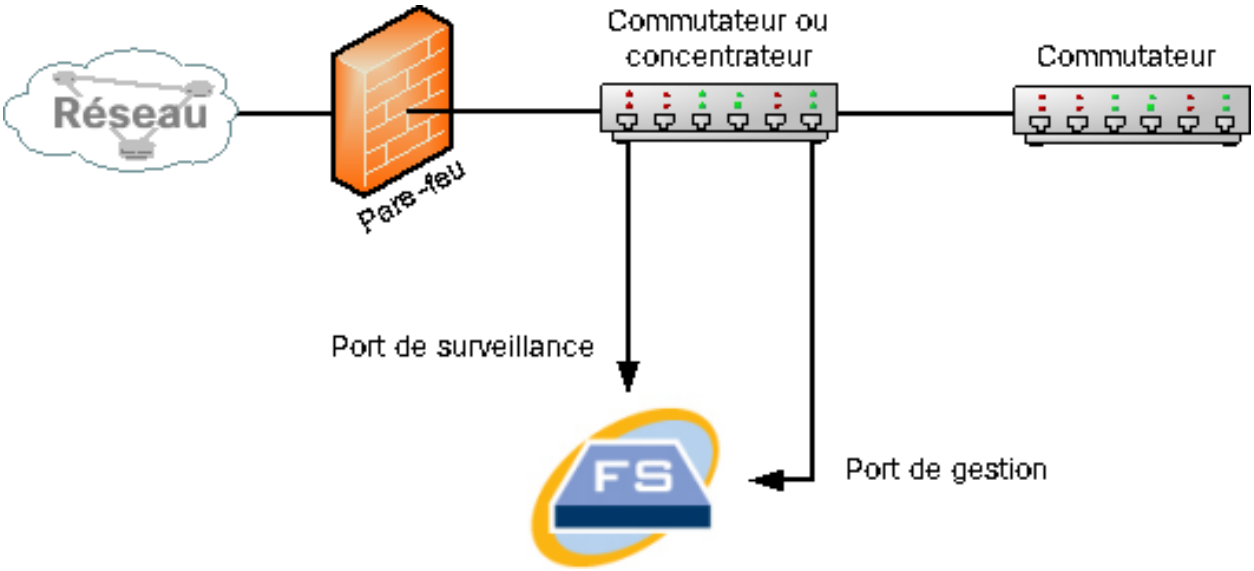
L'exemple ci-dessous montre l'utilisation d'un port TAP électrique. Le port de gestion doit être connecté au commutateur ou à un concentrateur du réseau surveillé. Cette configuration est similaire à la configuration qui surveille le trafic vers et depuis votre réseau.



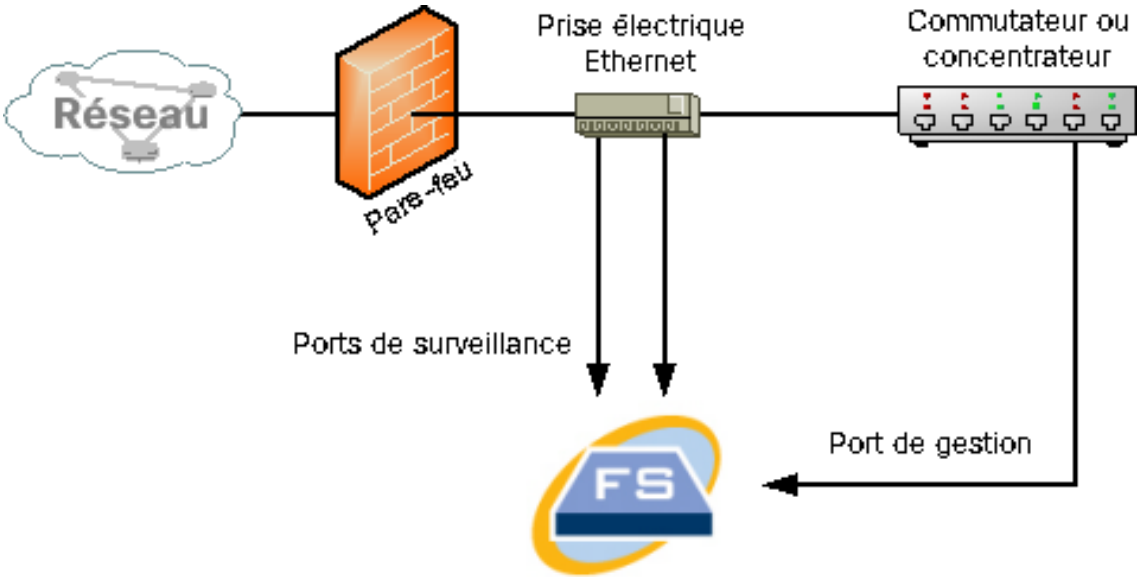
Si votre pare-feu effectue la traduction d'adresses réseau (NAT), vous pouvez uniquement observer les adresses qui sont sur le pare-feu.

Placement du capteur de flux à l'intérieur du pare-feu

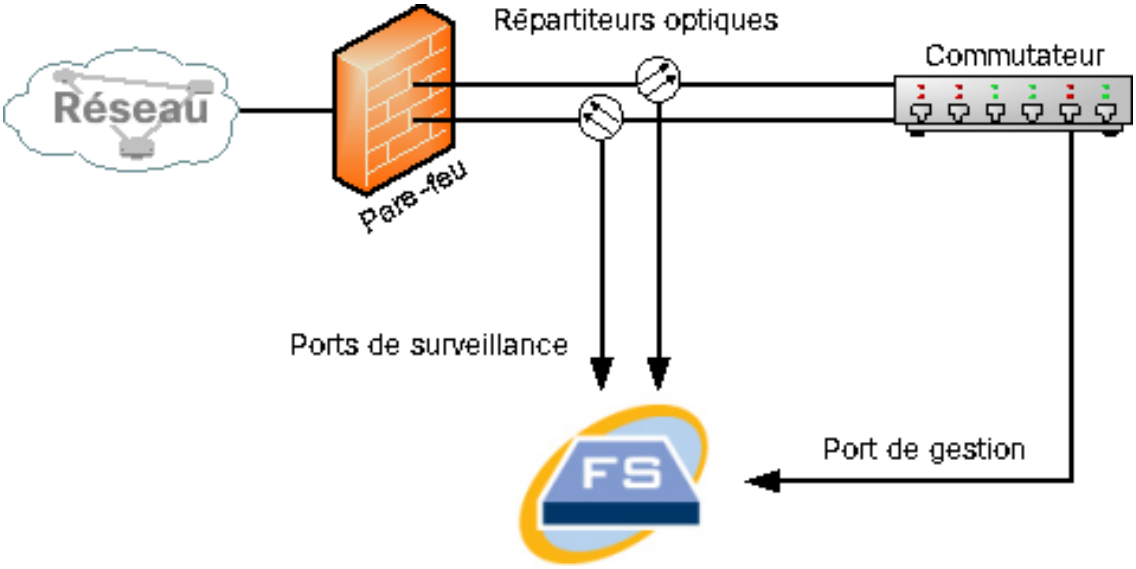
Pour surveiller le trafic entre les réseaux internes et un pare-feu, le capteur de flux doit pouvoir accéder à tout le trafic entre le pare-feu et les réseaux internes. Pour cela, configurez un port miroir qui reflète la connexion au pare-feu sur le commutateur principal. Assurez-vous que le port 1 du capteur de flux est connecté au port miroir, comme le montre l'illustration suivante :



Pour surveiller le trafic à l'intérieur du pare-feu à l'aide d'un port TAP, insérez le port TAP ou le répartiteur optique entre votre pare-feu et le commutateur ou concentrateur principal. Une configuration de port TAP est présentée ci-dessous.



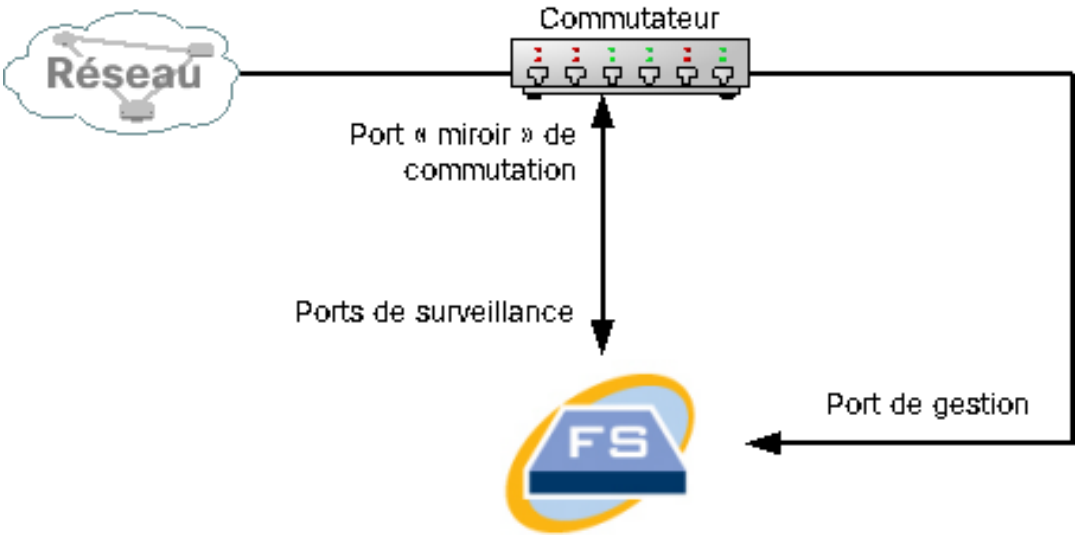
Une configuration de répartiteur optique est présentée ci-dessous.



Ports SPAN

Vous pouvez également connecter le capteur de flux à un commutateur. Cependant, étant donné qu'un commutateur ne répète pas tout le trafic sur chaque port, le capteur de flux ne fonctionnera pas correctement, sauf si le commutateur répète les paquets transmis vers et depuis un ou plusieurs ports de commutateur. Ce type de port de commutateur est parfois appelé un port miroir ou port SPAN.

L'illustration suivante montre comment obtenir cette configuration en connectant votre réseau au capteur de flux Stealthwatch via le port de gestion.



Dans cette configuration, vous devez configurer un port de commutateur (également appelé port miroir) pour répéter l'ensemble du trafic vers et depuis l'hôte copié par le port miroir. Le port 1 du capteur de flux doit être connecté à ce port miroir. Ainsi le capteur de flux surveille le trafic vers et depuis le réseau concerné et vers d'autres réseaux. Dans cet exemple, un réseau peut être constitué de certains ou de tous les hôtes connectés au commutateur.

Une méthode répandue pour configurer des réseaux sur un commutateur est de les délimiter dans des réseaux locaux virtuels (VLAN), qui sont logiques au lieu d'établir des connexions physiques d'hôtes. Si le port miroir est configuré pour refléter tous les ports sur un commutateur ou un VLAN, le capteur de flux surveille tout le trafic vers, depuis et au sein du réseau concerné, et les autres réseaux.

Dans tous les cas, nous vous recommandons de consulter la documentation du fabricant de votre commutateur afin de déterminer comment configurer le port miroir et quel trafic est répété vers celui-ci.

Préparation de l'installation

Avertissements relatifs à l'installation

Lisez le document Regulatory and Compliance Safety Information (Informations relatives à la conformité et à la sécurité) avant d'installer les appliances Stealthwatch x2xx.

Prenez en compte les avertissements suivants :

Énoncé 1071 : définition du symbole « Attention »

CONSIGNES DE SÉCURITÉ IMPORTANTES

⚠ Ce symbole indique un risque de danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Utilisez le numéro indiqué après chaque consigne de sécurité pour pouvoir retrouver sa traduction parmi les consignes relatives à ce périphérique.

CONSERVEZ CES INSTRUCTIONS.

Énoncé 1005 : disjoncteur

⚠ Un système de protection contre les risques de court-circuit (surintensité) doit être installé dans le bâtiment. Assurez-vous que la puissance nominale du dispositif de protection n'est pas supérieure à : 120 V, 15 A (USA), 250 V, 16 A (UE).

Énoncé 1 004 : consignes d'installation

⚠ Avant d'utiliser, d'installer ou de brancher le système sur la source d'alimentation, consultez les instructions d'installation.

Énoncé 12 : mise en garde relative à la déconnexion du module d'alimentation

⚠ Avant de travailler sur un châssis ou à proximité de modules d'alimentations, débranchez le câble d'alimentation des unités CA. Sur les unités CC, coupez l'alimentation au niveau du disjoncteur.

Énoncé 43 : mise en garde relative au retrait des bijoux

Avant d'utiliser un appareil raccordé au réseau électrique, retirez vos bijoux (bagues, colliers, montre, etc.). En cas de contact avec l'alimentation électrique et la mise à la terre, les objets métalliques peuvent chauffer et provoquer de graves brûlures ou se souder aux bornes.

Énoncé 94 : consigne de sécurité relative au bracelet

Au cours de la procédure, portez des bracelets de mise à la terre pour éviter d'endommager la carte par choc électrostatique. Pour éviter les risques d'électrocution, ne touchez pas le fond de panier directement avec les mains ni avec un outil métallique.

Énoncé 1045 : Avertissement relatif à la protection contre les courts-circuits

Un système de protection contre les courts-circuits (surintensité) doit être installé dans le bâtiment accueillant ce produit. Installez-le uniquement conformément aux réglementations nationales et locales.

Énoncé 1021 : circuit SELV

Pour prévenir tout risque de décharge électrique, ne connectez pas les circuits de sécurité de très basse tension (SELV) aux circuits de tension du réseau téléphonique (TNV). Les ports LAN comportent des circuits SELV et les ports WAN sont équipés de circuits TNV. Certains ports LAN et WAN utilisent des connecteurs RJ-45. Soyez prudent lors du branchement des câbles.

Énoncé 1 024 : conducteur de mise à la terre

Cet équipement doit être mis à la terre. N'endommagez jamais le conducteur de terre et n'utilisez pas l'équipement sans avoir préalablement installé un conducteur de terre adéquat. Contactez l'autorité de contrôle compétente ou un électricien si vous n'êtes pas sûr qu'une mise à la terre correcte a été effectuée.

Énoncé 1040 : mise au rebut du produit

La mise au rebut de ce produit doit être effectuée conformément aux réglementations nationales.

Énoncé 1074 : conformité aux codes de réglementation électrique régionaux et nationaux

L'installation de l'équipement doit être conforme aux réglementations électriques locales et nationales en vigueur.

Énoncé 19 : mise en garde relative à l'alimentation TN

Ce périphérique est conçu pour fonctionner avec des systèmes d'alimentation TN.

Consignes d'installation

Prenez en compte les avertissements suivants :

Énoncé 1047 : prévention de la surchauffe

Afin d'éviter toute surchauffe du système, ne l'utilisez pas dans une pièce dont la température ambiante dépasse la valeur maximale recommandée de 5 à 35 °C (41 à 95 °F).

Énoncé 1 019 : périphérique de déconnexion principal

Comme il constitue le principal dispositif de déconnexion, l'ensemble fiche-prise doit être accessible à tout moment.

Énoncé 1005 : disjoncteur

Un système de protection contre les risques de court-circuit (surintensité) doit être installé dans le bâtiment. Assurez-vous que la puissance nominale du dispositif de protection n'est pas supérieure à : 120 V, 15 A (USA), 250 V, 16 A (UE).

Énoncé 1074 : conformité aux codes de réglementation électrique régionaux et nationaux

L'installation de l'équipement doit être conforme aux réglementations électriques locales et nationales en vigueur.

Énoncé 371 : câble d'alimentation et adaptateur CA

Lors de l'installation du produit, utilisez les câbles de connexion, les cordons d'alimentation et les adaptateurs ou batteries CA fournis ou indiqués. L'utilisation d'un autre câble/adaptateur peut entraîner un dysfonctionnement ou un incendie. La réglementation sur les matériaux et les appareils électriques interdit l'utilisation des câbles certifiés UL (portant le sigle « UL » ou « CSA »), mais non conformes aux normes en vigueur si le sigle « PSE » n'est pas apposé sur le cordon, pour tout autre appareil électrique que les produits conçus par CISCO.

Énoncé 1073 : aucune pièce réparable ni remplaçable par l'utilisateur

Le périphérique ne contient aucune pièce réparable ni remplaçable par l'utilisateur. Ne l'ouvrez pas.

Lorsque vous installez un châssis, suivez les instructions ci-dessous :

- Assurez-vous qu'il y a suffisamment d'espace autour du châssis pour permettre les opérations de maintenance et la circulation de l'air. La circulation de l'air dans le châssis s'effectue de l'avant à l'arrière.

  Pour garantir une circulation d'air adéquate, placez vos châssis dans un rack en utilisant les kits de rails. Si vous placez physiquement les unités l'une au-dessus de l'autre ou les empilez sans utiliser les kits de rails, cela risque de bloquer les orifices de ventilation sur le dessus de chaque châssis, ce qui peut entraîner une surchauffe, et par conséquent une accélération des ventilateurs et une plus grande consommation électrique. Nous vous recommandons de monter vos châssis sur les kits de rails lorsque vous les installez dans le rack, car les kits de rails assurent l'espacement minimal nécessaire entre les châssis. Aucun espacement supplémentaire entre les châssis n'est requis lorsque vous les montez en utilisant les kits de rails.

- Veillez à ce que la climatisation maintienne les châssis à une température de 5 à 35 °C (41 à 95 °F).
- Assurez-vous que l'armoire ou le rack respecte les conditions relatives à l'utilisation de racks.
- Assurez-vous que l'alimentation du site respecte les conditions relatives à l'alimentation indiquées dans la notice technique de votre appliance. Le cas

échéant, vous pouvez utiliser un UPS pour protéger votre installation contre les pannes de courant.

> Évitez les types de systèmes UPS qui utilisent la technologie ferrorésonante. Ces types d'UPS risquent de devenir instables avec les systèmes qui présentent d'importantes variations de consommation électrique en raison d'un trafic de données fluctuant.

Consignes de sécurité

Lisez les informations suivantes pour assurer votre sécurité et protéger le châssis. Étant donné que ces informations ne couvrent pas toutes les situations potentiellement dangereuses dans votre environnement de travail, soyez vigilant et faites preuve de bon sens en toutes circonstances.

Respectez les consignes de sécurité suivantes :

- Maintenez la zone dégagée et exempte de poussière avant, pendant et après l'installation.
- Tenez les outils à l'écart des zones de passage afin d'éviter de trébucher.
- Ne portez pas de vêtements amples ou de bijoux, notamment des boucles d'oreille, des bracelets ou des colliers susceptibles de se coincer dans le châssis.
- Portez des lunettes de sécurité si vous travaillez dans des conditions présentant un risque pour les yeux.
- Ne faites rien qui soit susceptible de présenter un danger pour autrui ou qui puisse rendre le matériel dangereux.
- Ne tentez pas de soulever seul un objet trop lourd pour une personne.

Précautions de sécurité en présence d'électricité

> Avant de travailler sur un châssis, assurez-vous que le câble d'alimentation est débranché.

Respectez les consignes suivantes lorsque vous travaillez sur un équipement alimenté électriquement :

- Ne travaillez pas seul s'il existe des dangers potentiels sur votre lieu de travail.
- Vérifiez systématiquement que l'alimentation est déconnectée.

- Repérez les éventuels dangers présents dans votre zone de travail, tels que des sols humides, des câbles de rallonge non mis à la terre, des câbles d'alimentation endommagés et des prises de terre de sécurité manquantes.
- En cas d'accident électrique :
    - Soyez extrêmement prudent, ne devenez pas une victime vous-même.
    - Mettez le système hors tension.
    - Si possible, envoyez une autre personne demander de l'assistance médicale. Si cela s'avère impossible, évaluez l'état de la victime et demandez de l'aide.
    - Déterminez si vous devez pratiquer un bouche-à-bouche ou un massage cardiaque et donnez les soins requis.
- Utilisez le châssis conformément à ses caractéristiques électriques et respectez les instructions d'utilisation.

Éviter tout dommage par choc électrostatique

Les décharges électrostatiques se produisent en cas de manipulation incorrecte des composants électroniques. Elles peuvent endommager l'équipement et les circuits électriques, ce qui risque d'entraîner des dysfonctionnements ou une panne généralisée de votre équipement.

Suivez toujours les procédures de protection contre les décharges électrostatiques lorsque vous retirez ou remplacez des composants. Veillez à raccorder électriquement le châssis à une prise de terre. Portez un bracelet antistatique et vérifiez qu'il est bien en contact avec votre peau. Connectez la pince de mise à la terre à une surface non peinte du cadre du châssis afin de diriger en toute sécurité les tensions de décharge électrostatique vers la terre. Pour obtenir une bonne protection contre les chocs ou dommages causés par les décharges électrostatiques, vous devez vérifier que le bracelet de protection et le câble fonctionnent correctement. Si aucun bracelet de protection n'est disponible, reliez-vous à la terre en touchant la partie en métal du châssis.

Pour des raisons de sécurité, vérifiez régulièrement la valeur de résistance du bracelet de protection, qui doit être comprise entre 1 et 10 mégohms (Mohm).

Environnement du site

Pour éviter les défaillances matérielles et réduire les risques de pannes liés aux facteurs environnementaux, planifiez soigneusement l'agencement du site et l'emplacement des équipements. Si votre équipement subit des pannes ou des erreurs graves dont la fréquence est particulièrement élevée, les observations qui suivent peuvent vous aider à isoler leur cause et à prévenir de futurs problèmes.

Considérations en matière d'alimentation électrique

Lorsque vous installez le châssis, tenez compte des points suivants :

- Vérifiez l'alimentation sur le site avant d'installer le châssis pour vous assurer qu'elle ne présente aucun pic de tension et n'émet aucun bruit. Le cas échéant, installez un conditionneur d'énergie pour garantir une tension d'alimentation et des niveaux de puissance électrique adéquats en entrée de l'appliance.
- Mettez le site à la terre afin d'éviter les dommages causés par la foudre et les surtensions.
- L'utilisateur ne peut pas sélectionner de plage de fonctionnement sur le châssis. Consultez l'étiquette sur le châssis pour connaître la puissance d'entrée de l'équipement.
- Plusieurs types de câbles d'alimentation CA sont disponibles pour l'appliance ; vérifiez que vous disposez du type adapté à votre site.
- Si vous utilisez deux modules d'alimentation redondants (1+1), nous vous recommandons d'utiliser des circuits électriques indépendants pour chacun d'eux.
- Dans la mesure du possible, installez une source d'alimentation sans interruption sur votre site.

Conditions à prendre en compte pour la configuration en rack

Tenez compte de ce qui suit pour planifier une configuration en rack :

- Si vous montez un châssis dans un rack ouvert, assurez-vous que le cadre du rack ne bloque pas les orifices d'entrée et d'évacuation d'air.
- Assurez-vous que les racks fermés disposent d'une ventilation adéquate. Veillez également à ne pas surcharger le rack, car chaque unité génère de la chaleur. Un bâti fermé doit être doté de fentes d'aérations sur les côtés et d'un ventilateur pour permettre la circulation d'air de refroidissement.
- Dans un rack fermé doté d'un ventilateur supérieur, la chaleur générée par l'équipement situé dans la partie inférieure du rack peut remonter vers les ports d'entrée de l'équipement situé juste au-dessus. Assurez-vous que la circulation d'air est suffisante dans la partie inférieure du rack.
- Des déflecteurs peuvent aider à isoler l'air évacué de l'air entrant, ce qui permet également de faire circuler l'air de refroidissement dans le châssis. Le placement idéal des déflecteurs dépend de la circulation de l'air dans le rack. Essayez différentes dispositions pour positionner correctement les déflecteurs.

Installation

Cette section concerne l'installation des appliances dans votre environnement. Elle comprend :

- **Montage de votre appliance**
- **Connexion de votre appliance au réseau**
- **Connexion à l'appliance**
- **Définition des paramètres réseau à l'aide de l'assistant de configuration initiale**

Montage de votre appliance

Vous pouvez monter des appliances Stealthwatch directement dans une armoire ou un rack de 19 pouces standard, dans une autre armoire appropriée ou sur une surface plane. Lorsque vous installez une appliance dans une armoire ou un rack, suivez les instructions incluses dans les kits de montage de rails. Pour déterminer où placer une appliance, prévoyez suffisamment d'espace à l'avant et l'arrière de l'appliance en tenant compte de ce qui suit :

- Les indicateurs en façade doivent être clairement lisibles.
- L'accès aux ports à l'arrière est suffisant et permet d'effectuer un câblage sans restrictions.
- La prise d'alimentation du panneau arrière est à proximité d'une source d'alimentation AC conditionnée.
- L'air circule librement autour de l'appliance et à travers les orifices.

Matériel fourni avec l'appliance

Le matériel suivant est fourni avec les appliances Stealthwatch :

- Cordon d'alimentation CA
- Touches d'accès (pour la plaque de la face avant)
- Kit de rails pour le montage en rack ou étriers de montage pour les plus petites appliances
- Pour le collecteur de flux modèle 5210 un câble SFP de 10 Gbit

Matériel supplémentaire requis

Prévoyez le matériel supplémentaire suivant :

- Vis de fixation pour un rack standard de 19 pouces
- Source d'alimentation sans interruption (UPS) pour chaque appliance que vous installez
- Pour une configuration locale (facultatif), utilisez l'une des méthodes suivantes :
    - Ordinateur portable avec un câble vidéo et un câble USB (pour le clavier)
    - Moniteur vidéo avec un câble vidéo et un clavier avec un câble USB

Connexion de votre appliance au réseau

Utilisez la même procédure pour connecter chaque appliance au réseau. La connexion diffère selon le type d'appliance dont vous disposez.

> ⚠ Ne mettez pas à jour le BIOS de l'appliance, car cela pourrait entraîner un dysfonctionnement.

Pour obtenir des informations spécifiques sur chaque appliance, reportez-vous aux notices techniques Stealthwatch.

> ⓘ L'ensemble du matériel de la gamme Cisco x2xx utilise la même plateforme UCS (UCSC-C220-M5SX), à l'exception du collecteur de flux 5210 (base de données), qui utilise la plateforme UCSC-C240-M5SX. Les variations dans les appliances sont la carte réseau, le processeur, la mémoire, le stockage et le niveau RAID.

> ⓘ Le collecteur de flux 5210 se compose de deux serveurs connectés (moteur et base de données) afin qu'ils fonctionnent comme une même appliance. De ce fait, l'installation diffère légèrement d'autres appliances. Tout d'abord, connectez-les ensemble directement avec un câble d'interconnexion à attache directe SFP+ 10G. Ensuite, connectez-les à votre réseau.

Pour connecter votre appliance à votre réseau :

1. Connectez un câble Ethernet au port de gestion, à l'arrière de l'appliance.
2. Connectez au moins un port de moniteur pour les capteurs de flux et les appliances UDP Director.

   Pour la haute disponibilité des appliances UDP Director, reliez celles-ci avec des câbles croisés. Connectez le port eth2 d'une des deux appliances UDP Director au port eth2 de la seconde appliance UDP Director. De même, connectez les ports eth3 des deux appliances UDP Director avec un second câble croisé. Il peut s'agir

d'un câble fibre ou cuivre.

Tenez compte de l'étiquette Ethernet (eth2, eth3, etc.) pour chaque port. Ces étiquettes correspondent aux interfaces réseau (eth2, eth3, etc.) qui sont indiquées sur la page d'accueil de l'interface d'administration de l'appliance où vous pouvez les configurer.

3. Connectez l'autre extrémité des câbles Ethernet au commutateur de votre réseau.
4. Branchez les cordons d'alimentation au module d'alimentation. Certaines appliances ont deux connexions d'alimentation : module d'alimentation 1 et module d'alimentation 2.

Connexion à l'appliance

Cette section décrit comment vous connecter à votre appliance afin de modifier les mots de passe utilisateur par défaut.

Vous pouvez vous connecter à l'appliance de deux manières :

- avec un clavier et un moniteur
- avec un ordinateur portable (et un émulateur de terminal)

Pour les nouvelles appliances, SSH est désactivé. Vous devez vous connecter à l'interface web d'administration de l'appliance pour l'activer.

Se connecter avec un clavier et un moniteur

Pour configurer l'adresse IP localement, procédez comme suit :

1. Branchez le câble d'alimentation à l'appliance.
2. Poussez le bouton d'alimentation pour allumer l'appliance. Attendez qu'elle démarre complètement. N'interrompez pas le processus de démarrage.

> Vous devrez peut-être retirer la façade pour permettre l'alimentation.
>
> Les ventilateurs d'alimentation s'activent sur certains modèles alors que le système n'est pas sous tension. Vérifiez que le voyant sur la façade est allumé.
>
> Veillez à connecter l'appliance à un module d'alimentation sans interruption (UPS). Le module d'alimentation nécessite du courant, sinon le système affiche une erreur.

3. Connectez le clavier :

- Si vous disposez d'un clavier standard, branchez-le au connecteur de clavier standard.
- Si vous disposez d'un clavier USB, branchez-le à un connecteur USB.

4. Branchez le câble vidéo au connecteur vidéo. L'invite de connexion s'affiche.
5. Poursuivez avec la section **Définition des paramètres réseau à l'aide de l'assistant de configuration initiale**.

Se connecter avec un ordinateur portable

Vous pouvez également vous connecter à l'appliance avec un ordinateur portable équipé d'un émulateur de terminal.

Pour vous connecter à une appliance avec un ordinateur portable :

1. Connectez votre ordinateur portable à l'appliance en utilisant l'une des méthodes suivantes :

- Connectez un câble RS232 du connecteur du port série (DB9) sur votre ordinateur portable au port de console sur l'appliance.
- Connectez un câble croisé du port Ethernet sur votre ordinateur portable au port de gestion sur l'appliance.

2. Branchez le câble d'alimentation à l'appliance.
3. Poussez le bouton d'alimentation pour allumer l'appliance. Attendez qu'elle démarre complètement. N'interrompez pas le processus de démarrage.

> Vous devrez peut-être retirer la façade pour permettre l'alimentation.
>
> Les ventilateurs d'alimentation s'activent sur certains modèles alors que le système n'est pas sous tension. Vérifiez que le voyant sur la façade est allumé. Veillez à connecter l'appliance à un module d'alimentation sans interruption (UPS). Le module d'alimentation nécessite du courant, sinon le système affiche une erreur.

4. Sur l'ordinateur portable, établissez une connexion à l'appliance.

   Vous pouvez utiliser tout émulateur de terminal disponible pour communiquer avec l'appliance.

5. Appliquez les paramètres suivants :

   - BPS : 115200
   - Bits de données : 8
   - Bit d'arrêt : 1
   - Parité : aucune
   - Contrôle de flux : aucun

   L'écran de connexion et l'invite de connexion sont affichés.

6. Poursuivez avec la section suivante, **Définition des paramètres réseau à l'aide de l'assistant de configuration initiale**.

Définition des paramètres réseau à l'aide de l'assistant de configuration initiale

Après vous être connecté à l'appliance, utilisez l'assistant de configuration initiale pour configurer les paramètres réseau, notamment les adresses IP. Notez les éléments suivants :

- Si vous déployez une console SMC 2210 ou un collecteur de flux 4210 avec un data store, vous pouvez non seulement configurer les adresses IP, mais également la console SMC ou le collecteur de flux pour une utilisation avec le data store, ainsi que le type de port physique dont il se sert pour le port de gestion `eth0`.

  > ⚠ Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez plus changer ce paramètre dans la configuration de l'appliance. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option uniquement si vous prévoyez de déployer un data store sur votre réseau.

- Si votre appliance est un nœud de données, vous pouvez configurer le type de port physique qu'il utilise pour le port de gestion `eth0`, ainsi que l'adresse IP et les informations connexes pour le canal de port `eth2` ou `eth2`/`eth3` pour les communications du nœud de données.

Consultez le Guide de déploiement et de configuration du matériel du data store Stealthwatch pour en savoir plus sur l'installation des appliances SMC 2210, FC 4210 et des nœuds de données.

Après avoir configuré les adresses IP et les ports, modifiez les mots de passe utilisateur.

> La première fois que vous accédez à la configuration du système, l'assistant de configuration initiale démarre et vous guide tout au long de la configuration initiale de l'appliance. Si vous quittez la configuration initiale avant la fin de l'assistant, la prochaine fois que vous accéderez à la configuration du système, l'assistant de configuration initiale s'ouvrira de nouveau.

En fonction de votre appliance, accédez à la section suivante :

- **Appliances compatibles avec le data store (SMC 2210, FC 4210)**
- **Configuration générale de l'appliance Stealthwatch**
- **Configuration du nœud de données**

Configuration générale de l'appliance Stealthwatch

Pour toutes les appliances, à l'exception des nœuds de données, de la console SMC 2210 et de la console FC 4210, la configuration initiale affiche la configuration suivante :

- Configurer l'adresse IP et les informations de gestion de l'appliance

Configurer l'adresse IP et les informations de gestion de l'appliance :

Configurez l'adresse IP de gestion eth0 de votre appliance et les informations connexes dans l'assistant de configuration initiale. Pour la plupart des appliances, il s'agit de la première configuration de l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, accédez à la section Configuration du nœud de données.
- Si vous configurez une console SMC ou un collecteur de flux compatible avec le data store, accédez à la section Appliances compatibles avec le data store (SMC 2210, FC 4210).
- Si vous configurez une autre appliance Stealthwatch, commencez par l'étape 1.

Procédure

1. Connectez-vous au programme de configuration du système :
    - Si vous configurez une appliance compatible avec un nœud de données ou un data store, saisissez `root`, puis appuyez sur la touche **Entrée**. Si vous configurez toute autre appliance, saisissez `sysadmin`, puis appuyez sur la touche **Entrée**.

      > Les autorisations `root` sont requises pour configurer correctement le data store et sa compatibilité.

    - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
    - À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.
2. S'il s'agit de la configuration initiale du système sur cette appliance, l'assistant de configuration initiale démarre.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Spécifiez l'**adresse IP** de cette appliance.
4. Spécifiez le **masque réseau** du réseau.
5. Saisissez une adresse de **passerelle** comme adresse IP de cette appliance.
6. Spécifiez l'adresse de **diffusion** de l'appliance.
7. Spécifiez le **nom d'hôte** de l'appliance.
8. Spécifiez le **domaine** de l'appliance.
9. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

   Il s'agit de la dernière option de configuration de l'assistant de configuration initiale. Votre appliance redémarre et les modifications sont appliquées. Une fois que c'est fait, la page de connexion s'ouvre.

Étape(s) suivante(s)

- Modifiez les mots de passe utilisateur. Reportez-vous à la section **Modification du mot de passe de l'utilisateur Sysadmin** pour en savoir plus.

Appliances compatibles avec le data store (SMC 2210, FC 4210)

Pour le SMC 2210 et le FC 4210, l'assistant de configuration initiale affiche la configuration suivante :

1. Configurer le port physique de gestion eth0
2. Configurer l'adresse IP et les informations de gestion de l'appliance
3. Configurer la compatibilité du data store
4. Configurer l'utilisation de Cisco Security Analytics and Logging (on-premise)

> ⚠ Si vous devez effectuer un déploiement de Stealthwatch avec un data store, ne suivez pas les instructions de ce guide. Suivez les instructions du Guide d'installation du matériel des appliances Stealthwatch x2xx (avec data store).

Configurer le port physique de gestion eth0

Si vous configurez une console SMC ou un collecteur de flux compatible avec un data store et déployez un data store, vous pouvez éventuellement configurer `eth0` en tant que port DAC SFP+ plutôt que le port cuivre BASE-T par défaut. Pour ces appliances, il s'agit de la première configuration de l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, ou une console SMC ou un collecteur de flux compatible avec un data store, consultez la notice technique Stealthwatch de votre appliance pour obtenir des informations sur les ports SFP+ et BASE-T pris en charge.
- Si vous configurez un nœud de données, accédez à la section Configuration du nœud de données.
- Si vous configurez une autre appliance Stealthwatch outre les appliances compatibles avec un data store, reportez-vous à la section Configuration générale de l'appliance Stealthwatch.

Procédure

1. Connectez-vous au programme de configuration du système :
   - Tapez **root**, puis appuyez sur **Entrée**.

     > ⓘ Les autorisations `root` sont requises pour configurer correctement la compatibilité du data store.

   - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
   - À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.

2. Si vous accédez pour la première fois à la configuration du système sur cette appliance, l'assistant de configuration initiale démarre et la configuration de l'ordre des ports s'affiche. Passez à l'étape 5.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Dans le menu de configuration du système, sélectionnez **Network** (Réseau), puis appuyez sur **Entrée**.
4. Sélectionnez **Port Order** (Ordre des ports), puis appuyez sur Entrée.
5. Les options suivantes sont disponibles :
   - Sélectionnez **LOM** pour configurer votre appliance pour qu'elle utilise un port cuivre BASE-T pour eth0.
   - Sélectionnez **SFP+** pour configurer votre appliance afin qu'elle utilise un port fibre SFP+ pour eth0.
6. Sélectionnez **OK** pour confirmer la sélection.

Étape(s) suivante(s)

- Configurez l'adresse IP et les informations de gestion du port de gestion eth0. Reportez-vous à la procédure suivante.

Configurer l'adresse IP et les informations de gestion de l'appliance :

Configurez l'adresse IP de gestion eth0 de votre appliance et les informations connexes dans l'assistant de configuration initiale. Pour les appliances compatibles avec un data store, cette configuration a lieu après la configuration du port de gestion physique eth0.

Avant de commencer

- Si vous configurez une console SMC ou un collecteur de flux compatible avec un data store, après avoir configuré l'ordre des ports, l'assistant de configuration initiale affiche la configuration `eth0`. Passez à l'étape 3.

Procédure

1. Connectez-vous au programme de configuration du système :
   - Si vous configurez une appliance compatible avec un data store, saisissez `root`, puis appuyez sur la touche **Entrée**.

> Les autorisations `root` sont requises pour configurer correctement le data store et sa compatibilité.

- Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
- À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.

2. S'il s'agit de la configuration initiale du système sur cette appliance, l'assistant de configuration initiale démarre.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Spécifiez l'**adresse IP** de cette appliance.
4. Spécifiez le **masque réseau** du réseau.
5. Saisissez une adresse de **passerelle** comme adresse IP de cette appliance.
6. Spécifiez l'adresse de **diffusion** de l'appliance.
7. Spécifiez le **nom d'hôte** de l'appliance.
8. Spécifiez le **domaine** de l'appliance.
9. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

Étape(s) suivante(s)

- Configurez l'appliance pour une utilisation sans data store. Reportez-vous à la procédure suivante pour plus d'informations.

Configurer l'utilisation du data store

Configurez votre console SMC 2210 ou FC 4210 pour qu'elle fonctionne avec un data store. Vos collecteurs de flux se connecteront au data store et votre SMC interrogera ce dernier.

> Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez plus changer ce paramètre dans la configuration de l'appliance. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option **uniquement si** vous prévoyez de déployer un data store sur votre réseau.

Si vous devez effectuer un déploiement de Stealthwatch avec un data store, ne suivez pas les instructions de ce guide. Suivez les instructions du Guide d'installation du matériel des appliances Stealthwatch x2xx (avec data store).

> Vous devez configurer tous vos SMC et collecteurs de flux pour une utilisation avec un data store, si vous déployez un data store. Vous ne pouvez pas configurer certains de vos collecteurs de flux pour qu'ils se connectent au data store et d'autres pour qu'ils se connectent directement au SMC.

Avant de commencer

- Si vous vous trouvez dans l'assistant de configuration initiale, la configuration du système indique la configuration du data store une fois terminée la configuration de l'adresse IP de l'appliance. Passez à l'étape 3.

Procédure

1. Dans le menu de configuration du système. Sélectionnez **Advanced** (Avancé), puis appuyez sur **Entrée**.
2. Sélectionnez **Data Store**, puis appuyez sur Entrée.
3. Sélectionnez **Yes** (Oui) pour configurer la compatibilité de votre appliance avec un data store.

   > Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez plus changer ce paramètre dans la configuration de l'appliance. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option **uniquement si** vous prévoyez de déployer un data store sur votre réseau.

4. Sélectionnez **OK** pour confirmer la sélection.

Étape(s) suivante(s)

- Configurez Analyses de sécurité et journalisation sur site. Reportez-vous à la procédure suivante pour plus d'informations.

Configurer l'utilisation de Analyses de sécurité et journalisation sur site

Configurez votre console SMC 2210 ou FC 4210 pour Analyses de sécurité et journalisation sur site, afin d'utiliser votre déploiement Stealthwatch pour stocker des informations sur les événements Firepower. Votre collecteur de flux intègre les informations sur les événements Firepower et les envoie au data store pour stockage. Vous pouvez ensuite interroger ces informations sur les événements Firepower à partir de

votre Console de gestion Stealthwatch ou Firepower Management Center.

Si vous configurez Analyses de sécurité et journalisation sur site, vous devez également installer l'application Analyses de sécurité et journalisation sur site sur votre Console de gestion Stealthwatch. Pour en savoir plus, reportez-vous au Guide d'intégration des événements Firepower : analyses de sécurité et connexion.

> ⚠ Lorsque vous choisissez de configurer votre console SMC ou collecteur de flux pour une utilisation avec Analyses de sécurité et journalisation sur site, vous ne pouvez plus mettre à jour la configuration de l'appliance pour modifier ce paramètre. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option **uniquement si** vous prévoyez d'utiliser Stealthwatch pour Analyses de sécurité et journalisation sur site afin de stocker les informations relatives à vos événements Firepower.

Avant de commencer

- Si vous vous trouvez dans l'assistant de configuration initiale, la configuration du système indique la configuration de Analyses de sécurité et journalisation sur site une fois terminée celle de l'utilisation du data store.

Procédure

1. Sélectionnez **Oui** pour activer Analyses de sécurité et journalisation sur site et intégrer les informations relatives aux événements de pare-feu pour votre déploiement Firepower. Notez que la collecte NetFlow sera désactivée sur votre collecteur de flux.

   > ⚠ Lorsque vous choisissez de configurer votre console SMC ou collecteur de flux pour une utilisation avec Analyses de sécurité et journalisation sur site, vous ne pouvez plus mettre à jour la configuration de l'appliance pour modifier ce paramètre. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option **uniquement si** vous prévoyez d'utiliser Stealthwatch pour Analyses de sécurité et journalisation sur site afin de stocker les informations relatives à vos événements Firepower.

2. Sélectionnez **Non** pour désactiver Analyses de sécurité et journalisation sur site. Vous pouvez intégrer NetFlow sur votre collecteur de flux. Vous ne pouvez pas intégrer les informations sur les événements de pare-feu à partir de votre déploiement Firepower.
3. Sélectionnez **OK** pour confirmer la sélection.

Il s'agit de la dernière option de configuration de l'assistant de configuration initiale. Votre appliance redémarre et les modifications sont appliquées. Une fois que c'est fait, la page de connexion s'ouvre.

Configuration du nœud de données

Pour les nœuds de données, l'assistant de configuration initiale affiche la configuration suivante :

1. Configurer le port physique de gestion eth0
2. Configurer l'adresse IP et les informations de gestion de l'appliance
3. Configurer eth2 et eth3 pour les communications entre les nœuds de données

Configurer le port physique de gestion eth0

Si vous configurez un nœud de données, vous pouvez éventuellement configurer `eth0` en tant que port cuivre BASE-T plutôt que le port DAC SFP+ par défaut. Pour ces appliances, il s'agit de la première configuration de l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, consultez la fiche technique Stealthwatch de votre appliance pour obtenir des informations sur les ports SFP+ et BASE-T pris en charge.
- Si vous configurez une console SMC ou un collecteur de flux compatible avec le data store, accédez à la section Appliances compatibles avec le data store (SMC 2210, FC 4210).
- Si vous configurez une autre appliance Stealthwatch outre les appliances compatibles avec un data store, reportez-vous à la section Configuration générale de l'appliance Stealthwatch.

Procédure

1. Connectez-vous au programme de configuration du système :
    - Tapez **root**, puis appuyez sur **Entrée**.

      > Les autorisations `root` sont requises pour configurer correctement la compatibilité du data store.

- Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
- À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.

2. Si vous accédez pour la première fois à la configuration du système sur cette appliance, l'assistant de configuration initiale démarre et la configuration de l'ordre des ports s'affiche. Passez à l'étape 5.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Dans le menu de configuration du système, sélectionnez **Network** (Réseau), puis appuyez sur **Entrée**.
4. Sélectionnez **Port Order** (Ordre des ports), puis appuyez sur Entrée.
5. Les options suivantes sont disponibles :
   - Sélectionnez **SFP+** pour configurer votre appliance afin qu'elle utilise un port fibre SFP+ pour eth0.
   - Sélectionnez **LOM** pour configurer votre appliance pour qu'elle utilise un port cuivre BASE-T pour eth0.
6. Sélectionnez **OK** pour confirmer la sélection.

Étape(s) suivante(s)

- Configurez l'adresse IP et les informations de gestion du port de gestion eth0. Reportez-vous à la procédure suivante.

Configurer l'adresse IP et les informations de gestion de l'appliance :

Configurez l'adresse IP de gestion eth0 de votre appliance et les informations connexes dans l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, après avoir configuré l'ordre des ports, l'assistant de configuration initiale affiche la configuration de gestion `eth0`. Passez à l'étape 3.

Procédure

1. Connectez-vous au programme de configuration du système :
    - Si vous configurez un nœud de données, saisissez `root`, puis appuyez sur la touche **Entrée**.

      > Les autorisations `root` sont requises pour configurer correctement le data store et sa compatibilité.

    - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
    - À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.
2. S'il s'agit de la configuration initiale du système sur cette appliance, l'assistant de configuration initiale démarre.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Spécifiez l'**adresse IP** de cette appliance.
4. Spécifiez le **masque réseau** du réseau.
5. Saisissez une adresse de **passerelle** comme adresse IP de cette appliance.
6. Spécifiez l'adresse de **diffusion** de l'appliance.
7. Spécifiez le **nom d'hôte** de l'appliance.
8. Spécifiez le **domaine** de l'appliance.
9. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

Étape(s) suivante(s)

- Configurez les informations de gestion des ports de communication du nœud de données. Reportez-vous à la section **Configurer eth2 et eth3 pour les communications entre les nœuds de données :** pour en savoir plus.

Configurer eth2 et eth3 pour les communications entre les nœuds de données :

Lors de la configuration d'un nœud de données, configurez le port de communication inter-nœuds de données avec une adresse IP non routable. Vous pouvez configurer l'une des options suivantes :

- `eth2`
- canal de port contenant `eth2` et `eth3`

> Vous devez attribuer des adresses IP non routables à partir du bloc CIDR `169.254.42.0/24`.

Avant de commencer

- Consultez la notice technique Stealthwatch de votre appliance pour plus d'informations sur les ports SFP+ `eth2` et `eth3`. Notez que `eth2` et `eth3` dépendent de la configuration de `eth0`.
- Si vous vous trouvez dans l'assistant de configuration initiale, la configuration du système affiche la configuration du canal de port `eth2` ou `eth2/eth3` une fois que vous avez terminé de configurer les informations de gestion `eth0` de l'appliance. Passez à l'étape 3.

Procédure

1. Dans le menu de configuration du système, sélectionnez **Network** (Réseau), puis appuyez sur **Entrée**.
2. Sélectionnez **Node Communications** (Communications du nœud), puis appuyez sur Entrée.
3. Sélectionnez la configuration du port de communication inter-nœuds de données. Les options suivantes sont disponibles :
    - Sélectionnez **Yes** (Oui) pour ajouter `eth2` et `eth3` en tant que canal de port pour les communications entre les nœuds de données.
    - Sélectionnez **No** (Non) pour utiliser `eth2` pour les communications entre les nœuds de données.
4. Saisissez une **adresse IP** non routable à partir du bloc CIDR `169.254.42.0/24` pour `eth2` ou le canal de port `eth2/eth3`.
5. Spécifiez un **masque réseau** de `255.255.255.0` pour cette adresse IP.
6. Saisissez une adresse de **passerelle** pour cette adresse IP.
7. Saisissez une adresse de **diffusion** pour cette adresse IP.
8. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

    Il s'agit de la dernière option de configuration de l'assistant de configuration initiale. Votre appliance redémarre et les modifications sont appliquées. Une fois que c'est fait, la page de connexion s'ouvre.

Étape(s) suivante(s)

- Modifiez les mots de passe utilisateur. Reportez-vous à la section **Modification du mot de passe de l'utilisateur Sysadmin** pour en savoir plus.

Modification du mot de passe de l'utilisateur Sysadmin

Pour que votre réseau soit sécurisé, modifiez le mot de passe sysadmin par défaut pour les appliances.

Modifier le mot de passe sysadmin :

Avant de commencer

- Connectez-vous à la console de l'appliance en tant que **sysadmin**.
- Accédez à la configuration du système.

Procédure

1. Dans le menu de configuration du système, sélectionnez **Password** (Mot de passe), puis appuyez sur **Entrée**.

   Si vous modifiez la liste des hôtes approuvés par défaut, veillez à ce que chaque appliance Stealthwatch dans votre déploiement soit incluse dans cette liste. Si ce n'est pas le cas, les appliances ne seront pas en mesure de communiquer entre elles.

   Une invite pour le mot de passe actuel s'affiche sous le menu.
2. Saisissez le mot de passe actuel et appuyez sur **Entrée**.

   L'invite pour un nouveau mot de passe s'affiche.
3. Saisissez le nouveau mot de passe et appuyez sur **Entrée**.

   Le mot de passe doit comporter entre 8 et 30 caractères alphanumériques sans espaces. Vous pouvez également utiliser les caractères spéciaux suivants : `$.~!@#%_=?:,{}()`
4. Saisissez de nouveau le mot de passe et appuyez sur **Entrée**.
5. Lorsque votre mot de passe est accepté, appuyez de nouveau sur **Entrée** pour revenir au menu de configuration du système.
6. Passez à la section suivante, **Modification du mot de passe de l'utilisateur root**.

Modification du mot de passe de l'utilisateur root

Après avoir modifié le mot de passe par défaut de l'utilisateur sysadmin, vous devez modifier le mot de passe de l'utilisateur root par défaut pour renforcer la sécurité de votre réseau.

Modifier le mot de passe de l'utilisateur root :

Avant de commencer

- Connectez-vous à la console de l'appliance en tant que **sysadmin**.
- Accédez à la configuration du système.

Procédure

1. Accédez au shell root.
2. Dans le menu Configuration du système, sélectionnez **Advanced** (Avancé), puis appuyez sur **Entrée**. Le menu Advanced s'affiche.
3. Sélectionnez **RootShell**, puis appuyez sur **Entrée**.

   Une invite de mot de passe pour l'utilisateur root s'affiche.
4. Saisissez le mot de passe de l'utilisateur root actuel et appuyez sur **Entrée**. L'invite du shell root s'affiche.
5. Saisissez **SystemConfig**, puis appuyez sur **Entrée**.

   Vous retournez au menu de configuration du système pour modifier le mot de passe de l'utilisateur root.
6. Sélectionnez **Password** (Mot de passe), puis appuyez sur **Entrée**. L'invite du mot de passe s'affiche sous le menu.
7. Saisissez le nouveau mot de passe de l'utilisateur root et appuyez sur **Entrée**. Une deuxième invite s'affiche.
8. Saisissez à nouveau le nouveau mot de passe de l'utilisateur root et appuyez sur **Entrée**.
9. Une fois que votre mot de passe est modifié, appuyez sur **Entrée**. Vous avez désormais modifié les mots de passe sysadmin et root par défaut. Vous retournez au menu de la console de configuration du système.
10. Cliquez sur **Cancel** (Annuler), puis appuyez sur **Entrée**. La console de configuration du système se ferme et l'invite du shell root s'affiche.

11. Saisissez **exit** et appuyez sur **Entrée**. L'invite de connexion s'affiche.
12. Appuyez sur **Ctrl + Alt** pour quitter l'environnement de la console.

Vous êtes maintenant prêt à configurer votre appliance. Pour configurer votre appliance, reportez-vous au **Guide de configuration Stealthwatch** correspondant à votre version logicielle. L'appliance x2xx est compatible avec les versions logicielles Stealthwatch 7.x.

Configuration de votre appliance

Vous êtes maintenant prêt à configurer votre appliance. Pour configurer votre appliance, reportez-vous au **Guide de configuration du système Stealthwatch** et au Guide de déploiement et de configuration du matériel du data store Stealthwatch pour votre version logicielle. L'appliance x2xx est compatible avec les versions logicielles Stealthwatch 7.x.

Informations de copyright