Cisco Stealthwatch

Installationshandbuch für die Serie x210

Table of Contents

Einführung

Übersicht

Dieses Handbuch erklärt die Installation der Hardware-Appliances der Stealthwatch-Serie x210. Es beschreibt die Stealthwatch-Komponenten und ihre Integration in das System, einschließlich der Integration von Flow Sensors. Diese Anleitung beschreibt auch die Montage und Installation der Stealthwatch-Hardware. Die Hardware der Serie x210 umfasst:

Appliance	**Teilenummer**
Stealthwatch Flow Collector 4210	ST-FC4210-K9
Stealthwatch Flow Collector 5210 Engine	ST-FC521010-E
Stealthwatch Flow Collector 5210-Datenbank	ST-FC521010-D
Stealthwatch Flow Sensor 1210	ST-FS121010-K9
Stealthwatch Flow Sensor 3210	ST-FS3210-K9
Stealthwatch Flow Sensor 4210	ST-FS4210-K9
StealthWatch Management Console 2210	ST-SMC221010-K9
Stealthwatch UDP Director 2210	ST-UDP221010-K9

Zielgruppe

Dieses Handbuch richtet sich an die Person, die für die Installation der Stealthwatch-Hardware verantwortlich ist. Wir gehen davon aus, dass Sie bereits über Grundkenntnisse in der Installation von Netzwerkgeräten verfügen (Flow Sensor, Flow Collector, UDP Director und Stealthwatch Management-Konsole).

Informationen zur Konfiguration von Stealthwatch-Appliances finden Sie im jeweiligen **Stealthwatch-Handbuch für die Installation und Konfiguration** für Ihre Softwareversion. Die Serie x210 ist kompatibel mit den Stealthwatch-Softwareversionen 7.x.

Hinweise zur Verwendung dieses Handbuchs

Neben zu dieser Einführung haben wir diesen Leitfaden in die folgenden Kapitel unterteilt:

Kapitel	Beschreibung
2 – **Überlegungen vor der Konfiguration**	Stealthwatch-Komponenten, ihre Platzierung und Konfiguration der Firewall für die Kommunikation
3 – **Vorbereitung der Installation**	Sicherheitsrichtlinien, Warnungen und Empfehlungen
4 – **Installation**	Montage und Installation der Stealthwatch-Hardware

Häufige Abkürzungen

Die folgenden Abkürzungen werden in diesem Handbuch verwendet:

Abkürzung	Beschreibung
DMZ	Demilitarisierte Zone (ein Perimeternetzwerk)
HTTPS	Hypertext Transfer Protocol (Secure)
ISE	Identity Services Engine
NIC	Netzwerkkarte
NTP	Network Time Protocol
PCIe	Peripheral Component Interconnect Express
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
TAP	Test Access Port
USV	Unterbrechungsfreie Stromversorgung
VLAN	Virtual Local Area Network

Vorbereitung der Installation

Installationswarnungen

Lesen Sie vor der Installation der Stealthwatch-Appliance der Serie x210 das Dokument Erfüllung gesetzlicher Auflagen und Sicherheitsinformationen.

Beachten Sie die folgenden Warnhinweise:

Anweisung 1071 – Definition der Warnhinweise

IMPORTANT SAFETY INSTRUCTIONS

⚠ This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE ANWEISUNGEN SICHER AUF.

Erklärung 1005 – Leitungsschutzschalter

⚠ Dieses Produkt ist für Gebäude mit Kurzschlusssicherung (Überstromschutz) gedacht. Stellen Sie sicher, dass der Nennwert der Schutzvorrichtung folgende Werte nicht überschreitet: USA 120 V, 15 A (EU: 250 V, 16 A)

Anweisung 1004 – Installationsanweisungen

⚠ Lesen Sie die Installationshinweise, bevor Sie das System nutzen, installieren oder an die Stromversorgung anschließen.

Anweisung 12 – Warnhinweis zum Trennen der Stromversorgung

⚠ Bevor Sie an einem Chassis oder in der Nähe von Netzteilen arbeiten, ziehen Sie von AC-Geräten das Netzkabel ab, oder trennen Sie bei DC-Geräten die Stromversorgung am Leitungsschutzschalter.

Anweisung 43 – Warnhinweis zum Ablegen von Schmuck

Bevor Sie an Geräten arbeiten, die mit Stromleitungen verbunden sind, legen Sie Ihren Schmuck ab (einschließlich Ringe, Halsketten und Uhren). Metallobjekte erhitzen sich bei der Verbindung mit Strom und Masse und können schwere Verbrennungen verursachen, oder das Metall kann mit den Terminals verschmelzen.

Anweisung 94 – Warnhinweis zu Armbändern

Tragen Sie bei diesem Verfahren Erdungsarmbänder, um Schäden an der Karte durch elektrostatische Entladungen zu vermeiden. Berühren Sie die Backplane nicht mit der Hand oder einem Metallwerkzeug, da Sie sonst einen Stromschlag bekommen können.

Erklärung 1045 – Kurzschlusssicherung

Dieses Produkt muss im Rahmen der Gebäudeinstallation mit einer Kurzschlusssicherung (Überstromschutz) versehen sein. Installieren Sie es nur in Übereinstimmung mit den nationalen und lokalen Verkabelungsvorschriften.

Anweisung 1021 – SELV-Schaltkreise

Zur Vermeidung von Stromschlägen sollten Sie keine Sicherheitskleinspannungs-Schaltkreise (SELV) an Telefonnetz-Schaltkreise (TNV) anschließen. LAN-Ports verfügen über SELV-Schaltkreise, WAN-Ports über TNV-Schaltkreise. In manchen Fällen verwenden sowohl LAN- als auch WAN-Ports RJ-45-Stecker. Gehen Sie beim Anschluss von Kabeln vorsichtig vor.

Erklärung 1024 – Erdungsleiter

Dieses Gerät muss geerdet sein. Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an die zuständige Inspektionsbehörde oder einen Elektriker.

Erklärung 1040 – Entsorgung des Produkts

Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.

Erklärung 1074 – Übereinstimmung mit örtlichen und nationalen elektrischen Richtlinien und Bestimmungen

Die Installation des Geräts muss in Übereinstimmung mit den örtlichen und nationalen elektrischen Richtlinien und Bestimmungen erfolgen.

Erklärung 19 – Warnung TN-Stromversorgung

Das Gerät ist mit TN-Stromversorgungssystemen kompatibel.

Installationsrichtlinien

Beachten Sie die folgenden Warnhinweise:

Erklärung 1047 – Überhitzungsschutz

Um das System vor Überhitzung zu schützen, vermeiden Sie dessen Verwendung in Bereichen, in denen die Umgebungstemperatur außerhalb des folgenden Bereichs liegt: 5 bis 35 °C.

Erklärung 1019 – Primäre Ausschaltvorrichtung

Die Stecker-Steckdosen-Kombination muss jederzeit zugänglich sein, da sie zum Ausschalten des Geräts dient.

Erklärung 1005 – Leitungsschutzschalter

Dieses Produkt ist für Gebäude mit Kurzschlusssicherung (Überstromschutz) gedacht. Stellen Sie sicher, dass der Nennwert der Schutzvorrichtung folgende Werte nicht überschreitet: USA 120 V, 15 A (EU: 250 V, 16 A)

Erklärung 1074 – Übereinstimmung mit örtlichen und nationalen elektrischen Richtlinien und Bestimmungen

Die Installation des Geräts muss in Übereinstimmung mit den örtlichen und nationalen elektrischen Richtlinien und Bestimmungen erfolgen.

Anweisung 371 – Netzkabel und Netzteil

Nutzen Sie für die Installation des Produkts die mitgelieferten oder vorgesehenen Verbindungskabel/Netzkabel/AC-Adapter/Batterien. Die Nutzung anderer Kabel oder Adapter kann Funktionsstörungen oder einen Brand verursachen. Das (japanische) Gesetz zur Sicherheit von Elektrogeräten und elektrischem Material verbietet die Nutzung von zertifizierten Kabeln (bei denen im Code „UL“ steht) für andere elektrische Geräte, als die von Cisco festgelegten Produkte. Diese müssen stattdessen das PSE-Zeichen auf dem Kabel aufweisen.

Erklärung 1073 – Keine vom Benutzer zu wartenden Teile

Innen befinden sich keine vom Benutzer zu wartenden Teile. Nicht öffnen.

Beachten Sie bei der Installation des Chassis die folgenden Richtlinien:

- Stellen Sie sicher, dass um das Chassis herum genügend Platz für Wartungsarbeiten und für eine ausreichende Belüftung bleibt. Der Luftstrom im Chassis fließt von vorne nach hinten.

  Um einen einwandfreien Luftstrom zu gewährleisten, muss Ihr Chassis mit Gleitschienen-Sätzen montiert werden. Das Übereinanderstapeln der Einheiten oder das Stapeln ohne Verwendung der Gleitschienen-Sätze blockiert die Lüftungsöffnungen auf dem Chassis, was zu Überhitzung, höheren Lüfterdrehzahlen und einem höheren Stromverbrauch führen kann. Wir empfehlen Ihnen, Ihr Chassis beim Einbau in das Rack auf Gleitschienen zu montieren, da diese Schienen den erforderlichen Mindestabstand zwischen den Chassis gewährleisten. Bei der Montage mit Gleitschienen-Sätzen ist kein zusätzlicher Abstand zwischen den Chassis erforderlich.

- Stellen Sie sicher, dass die Klimaanlage das Chassis auf einer Temperatur von 5 bis 35 °C halten kann.
- Stellen Sie sicher, dass der Schrank oder das Rack den Rack-Anforderungen entspricht.
- Stellen Sie sicher, dass die Stromversorgung am Standort die im Datenblatt Ihrer Appliance aufgeführten Stromversorgungsbedingungen erfüllt. Sie können eine USV zum Schutz vor Stromausfällen verwenden (falls verfügbar).

Vermeiden Sie USV-Modelle mit Ferroresonanztechnologie. Diese USV-Modelle können bei der Verwendung mit solchen Systemen, die aufgrund von stoßartigen Datenverkehrsmustern erhebliche Schwankungen im Stromverbrauch aufweisen können, instabil werden.

Sicherheitshinweise

Beachten Sie zu Ihrer eigenen Sicherheit und zum Schutz des Chassis die folgenden Informationen. Darin werden möglicherweise nicht alle potenziell gefährlichen Situationen in Ihrer Arbeitsumgebung abgedeckt. Seien Sie daher wachsam, und lassen Sie stets Vorsicht walten.

Beachten Sie die folgenden Sicherheitsrichtlinien:

- Halten Sie den Bereich vor, während und nach der Installation sauber und staubfrei.
- Legen Sie Ihre Werkzeuge nicht in Gangflächen ab, wo Sie oder andere darüber stolpern könnten.
- Tragen Sie keine losen Kleidungsstücke oder Schmuck, wie Ohrringe, Armbänder oder Halsketten, die sich im Chassis verfangen könnten.
- Tragen Sie bei Arbeiten unter Bedingungen, die möglicherweise die Augen gefährden, eine Schutzbrille.
- Unterlassen Sie alles, was eine Gefahr für Personen darstellen kann oder die Sicherheit des Geräts beeinträchtigt.
- Versuchen Sie niemals, ein Objekt anzuheben, das für eine Person allein zu schwer ist.

Sicherheit bei Arbeiten mit Elektrizität

> ⚠ Bevor Sie an einem Chassis arbeiten, stellen Sie sicher, dass das Netzkabel abgezogen ist.

Befolgen Sie bei Arbeiten an mit elektrischem Strom betriebenen Geräten diese Richtlinien:

- Arbeiten Sie nicht allein, wenn an Ihrem Arbeitsplatz potenziell gefährliche Bedingungen vorhanden sind.
- Nehmen Sie niemals an, dass die Stromversorgung getrennt ist. Überprüfen Sie dies stets.
- Suchen Sie sorgfältig nach möglichen Gefahren in Ihrem Arbeitsbereich, z. B. feuchten Böden, nicht geerdeten Verlängerungskabeln, durchgescheuerten Netzkabeln und fehlenden Schutzerdungen.
- Bei einem elektrischen Unfall:
  - Seien Sie vorsichtig, und werden Sie nicht selbst zum Opfer.
  - Trennen Sie die Stromversorgung des Systems.

    - Wenn möglich, bitten Sie eine andere Person, medizinische Betreuung zu leisten. Versuchen Sie andernfalls, den Zustand des Opfers einzuschätzen, und holen Sie dann Hilfe.
    - Bestimmen Sie, ob die Person Mund-zu-Mund-Beatmung oder eine Herzmassage benötigt; ergreifen Sie dann die geeigneten Maßnahmen.
- Verwenden Sie das Chassis mit der angegebenen Spannung und wie im Benutzerhandbuch angegeben.

Vermeidung von Schäden durch ESD

ESD tritt auf, wenn elektronische Komponenten nicht ordnungsgemäß genutzt werden. Dadurch können Geräte und elektrische Schaltkreise beschädigt werden und einen temporären oder vollständigen Ausfall Ihrer Geräte verursachen.

Beachten Sie immer die Vorgehensweisen zur Vermeidung von Schäden durch elektrostatische Entladung, wenn Sie Komponenten ausbauen und ersetzen. Stellen Sie sicher, dass das Chassis geerdet ist. Verwenden Sie immer ein antistatisches Armband und stellen Sie guten Hautkontakt sicher. Verbinden Sie die Erdungsklemme mit einer unlackierten Fläche am Chassis-Rahmen, um ESD-Spannungen sicher zu erden. Zum zuverlässigen Schutz vor Beschädigungen durch ESD und vor Stromschlägen müssen das Armband und der Leiter wirksam funktionieren. Wenn kein Armband verfügbar ist, erden Sie sich durch Berühren des Metallteils am Chassis.

Überprüfen Sie zu Ihrem Schutz regelmäßig den Widerstandswert des antistatischen Armbands. Er sollte zwischen einem und 10 Megohm liegen.

Standortumgebung

Planen Sie das Layout des Standorts und die Positionen der Geräte sorgfältig, um Geräteausfälle zu vermeiden und die Wahrscheinlichkeit umgebungsbedingter Systemabschaltungen zu verringern. Sollte es bei Ihren derzeitigen Geräten zu Systemabschaltungen oder ungewöhnlich hohen Fehlerraten kommen, können Sie mithilfe dieser Empfehlungen die Ursache der Ausfälle lokalisieren und künftige Probleme vermeiden.

Überlegungen zur Stromversorgung

Beachten Sie bei der Installation des Chassis Folgendes:

- Vergewissern Sie sich vor der Installation des Chassis, dass die Stromversorgung am Standort frei von Spitzen und Störungen ist. Installieren Sie bei Bedarf ein Netzschutzgerät, um ein angemessenes Spannungs- und Stromniveau in der Eingangsspannung der Appliance sicherzustellen.

- Installieren Sie eine geeignete Erdung für den Standort, um Schäden durch Blitzschlag und Stromanstiege zu vermeiden.
- Der Betriebsbereich des Chassis kann nicht durch den Benutzer festgelegt werden. Entnehmen Sie die korrekten Eingangsspannungsanforderungen der Appliance dem Etikett auf dem Chassis.
- Es stehen verschiedene Arten von Wechselstrom-Netzkabel für die Appliance zur Verfügung. Vergewissern Sie sich, dass Ihnen das korrekte Kabel für Ihren Standort vorliegt.
- Falls Sie doppelte redundante (1+1) Netzteile verwenden, empfehlen wir Ihnen die Nutzung unabhängiger Stromkreise für jedes der Netzteile.
- Installieren Sie, falls möglich, eine unterbrechungsfreie Stromversorgung für Ihren Standort.

Überlegungen zur Rack-Konfiguration

Beachten Sie beim Planen der Rack-Konfiguration die folgenden Punkte:

- Wenn Sie ein Chassis in einem offenen Rack montieren, stellen Sie sicher, dass der Rack-Rahmen die Ein- und Auslassöffnungen nicht blockiert.
- Stellen Sie sicher, dass geschlossene Racks ausreichend belüftet werden. Stellen Sie sicher, dass das Rack nicht zu voll ist, da jedes Chassis Wärme erzeugt. Ein geschlossenes Rack sollte seitliche Luftschlitze und einen Lüfter haben, um Kühlluft zur Verfügung zu stellen.
- In einem geschlossenen Rack mit einem Lüfter oben kann die von Geräten im unteren Bereich des Racks erzeugte Wärme in die Einlassöffnungen der darüberliegenden Einheiten gezogen werden. Stellen Sie sicher, dass Einheiten im unteren Bereich des Racks ausreichend belüftet werden.
- Leitbleche können dazu beitragen, Abluft von der Ansaugluft zu trennen, was auch die Kühlluftzirkulation durch das Chassis verbessert. Die beste Platzierung der Leitbleche hängt von den Luftstrommustern im Rack ab. Probieren Sie verschiedene Varianten aus, um die beste Position für die Leitbleche zu finden.

Überlegungen zur Vorkonfiguration

Dieser Abschnitt enthält die Überlegungen, die Sie vor der Installation und Konfiguration Ihrer Stealthwatch-Appliances anstellen sollten. Es wird erklärt, wo Stealthwatch-Appliances platziert werden sollten und wie Sie sie in Ihr Netzwerk integrieren können. Enthalten sind:

Anmeldung mit dem CIMC-Standardkennwort

Der Cisco Integrated Management Controller (CIMC) ermöglicht den Zugriff auf die Serverkonfiguration und eine virtuelle Serverkonsole sowie die Überwachung des Hardwarezustands. Verwenden Sie das folgende Standardkennwort, um sich beim CIMC anzumelden: `password`.

Ändern Sie nach der Anmeldung das Standardpasswort, um die Sicherheit Ihres Netzwerks zu gewährleisten.

Über Stealthwatch-Appliances

Stealthwatch umfasst mehrere Hardware-Appliances, die Informationen über Ihr Netzwerk sammeln, analysieren und darstellen, um die Netzwerkleistung und -sicherheit zu verbessern. Dieser Abschnitt beschreibt die einzelnen Appliances der Stealthwatch-Serie x210.

> Weitere Informationen finden Sie in den Datenblättern der Appliances der Stealthwatch-Serie x210.

Stealthwatch Management Console 2210

Die Stealthwatch Management Console verwaltet, koordiniert, konfiguriert und organisiert alle Einzelkomponenten des Systems. Die Stealthwatch-Software ermöglicht Ihnen den Zugriff auf die Web-Benutzeroberfläche der Konsole von jedem Computer mit Webbrowser. Sie können problemlos auf Echtzeit-Sicherheits- und Netzwerkinformationen über kritische Segmente in Ihrem gesamten Unternehmen zugre-

ifen. Mit der Java-basierten Plattformunabhängigkeit ermöglicht die Stealthwatch Management Console Folgendes:

- Zentralisierte Verwaltung, Konfiguration und Berichterstellung für bis zu 25 Stealthwatch Flow Collectors
- Grafische Diagramme zur Visualisierung des Datenverkehrs
- Detaillierte Analyse zur Fehlerbehebung
- Konsolidierte und anpassbare Berichte
- Trendanalyse
- Leistungsüberwachung
- Sofortige Benachrichtigung über Sicherheitsprobleme

Stealthwatch Flow Collector 4210 und 5210

Der Stealthwatch Flow Collector sammelt NetFlow-, cFlow-, J-Flow-, Packeteer 2-, NetStream- und IPFIX-Daten, um einen verhaltensbasierten Netzwerkschutz zu bieten.

Durch Aggregierung von Hochgeschwindigkeits-Verhaltensdaten verschiedener Netzwerke oder Netzwerksegmente ermöglicht der Flow Connector End-to-End-Schutz und verbessert die Leistung über geografisch verteilte Netzwerke hinweg.

> Während der Flow Collector Daten empfängt, identifiziert er bekannte oder unbekannte Angriffe, internen Missbrauch und falsch konfigurierte Netzwerkgeräte, unabhängig von der Paketverschlüsselung oder -fragmentierung. Sobald Stealthwatch das Verhalten identifiziert hat, kann das System alle Maßnahmen ergreifen, die Sie gegebenenfalls für diese Art von Verhalten konfiguriert haben.

Stealthwatch Flow Sensor 1210, 3210, und 4210

Der Stealthwatch Flow Sensor ist eine Netzwerk-Appliance, die ähnlich wie eine herkömmliche Paketerfassungs-Appliance oder IDS funktioniert, indem sie an einen Switch Port Analyzer (SPAN), Mirror Port oder Ethernet Test Access Port (TAP) angeschlossen wird. Der Flow Sensor erhöht die Transparenz in den folgenden Netzwerkbereichen:

- Bereiche, in denen NetFlow nicht verfügbar ist
- Bereiche, in denen NetFlow verfügbar ist, Sie aber einen besseren Überblick über Leistungsmetriken und Paketdaten wünschen.

Wenn Sie den Flow Sensor auf einen beliebigen NetFlow v9-fähigen Flow Collector ausrichten, können Sie wertvolle detaillierte Datenverkehrsstatistiken von NetFlow

erhalten. In Kombination mit dem Stealthwatch Flow Collector bietet der Flow Sensor auch einen detaillierten Einblick in Leistungsmetriken und Verhaltensindikatoren. Diese Flow-Leistungskennzahlen geben Aufschluss über jede Round-Trip-Latenz, die durch das Netzwerk oder die serverseitige Anwendung verursacht wird.

Da der Flow Sensor auf Paketebene sichtbar ist, kann er die Round-Trip-Zeit (RTT), die Server-Reaktionszeit (SRT) und den Paketverlust für TCP-Sitzungen berechnen. Diese zusätzlichen Felder werden in die NetFlow-Datensätze integriert, die der Sensor an den Flow Collector sendet.

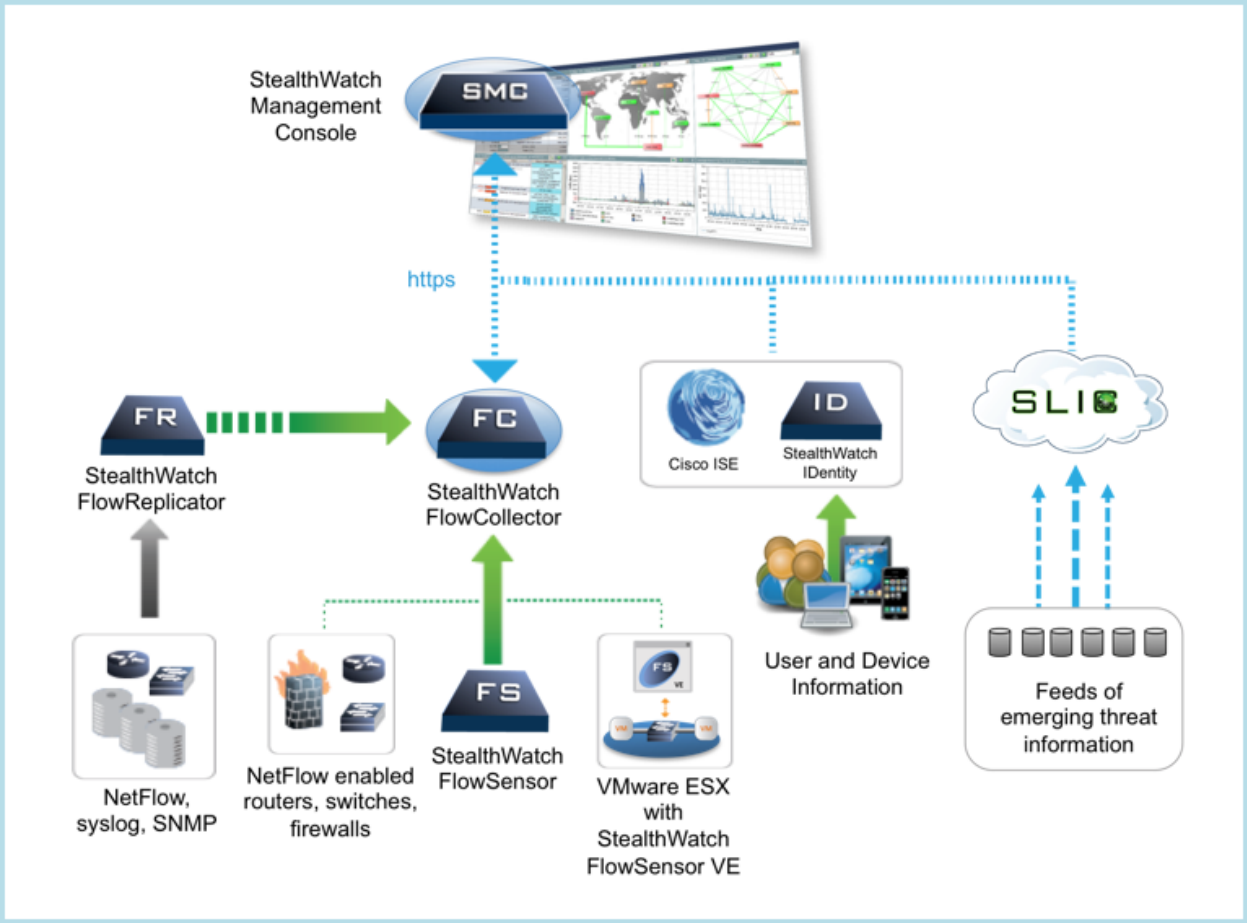
Stealthwatch UDP Director 2210

Der Stealthwatch UDP Director ist ein schneller, leistungsstarker UDP-Paketreplikator. Der UDP Director ist sehr hilfreich bei der Weiterverteilung von NetFlow-, sFlow-, syslog- oder Simple Network Management Protocol (SNMP)-Traps an verschiedene Collectors. Er kann Daten von jeder beliebigen verbindungslosen UDP-Anwendung empfangen und an verschiedene Ziele weiterleiten, wobei die Daten bei Bedarf dupliziert werden.

Wenn Sie die UDP Director High Availability (HA)-Konfiguration (Failover) verwenden, müssen Sie zwei UDP Director-Appliances über Crossover-Kabel verbinden. Spezifische Anweisungen finden Sie unter **Verbinden Ihrer Appliance mit dem Netzwerk**.

Platzierung Ihrer Appliances

Wie in der folgenden Abbildung dargestellt, können Sie Stealthwatch-Appliances strategisch so konfigurieren, dass sie die wichtigsten Netzwerksegmente im gesamten Netzwerk optimal abdecken, sei es im internen Netzwerk, am Perimeter oder in der DMZ.



Aufstellen der Stealthwatch Management Console

Installieren Sie die Stealthwatch Management-Konsole als Management-Gerät an einem Ort in Ihrem Netzwerk, der für alle Geräte zugänglich ist, die Daten an sie senden.

Wenn Sie für den Failover zwei Stealthwatch Management-Konsolen haben, empfehlen wir, die primäre und die sekundäre Konsole an getrennten physischen Orten zu installieren. Diese Strategie vereinfacht die Notfallwiederherstellung, falls erforderlich.

Aufstellen des Stealthwatch Flow Collector

Als Collector- und Überwachungsgerät sollte der Stealthwatch Flow Collector an einem Ort in Ihrem Netzwerk installiert werden, der für NetFlow- oder sFlow-Geräte, die die Daten an einen Flow Collector senden, sowie für alle Geräte, die Sie für den Zugriff auf die Management-Oberfläche verwenden möchten, zugänglich ist.

Wenn Sie einen Flow Collector außerhalb einer Firewall platzieren, empfehlen wir Ihnen, die Einstellung **Accept traffic from any exporter** (Datenverkehr von jedem Exporter akzeptieren) zu deaktivieren.

Platzieren des Stealthwatch Flow Sensors

Als passives Überwachungsgerät kann der Stealthwatch Flow Sensor an mehreren Stellen in Ihrem Netzwerk positioniert sein, um IP-Aktivitäten zu beobachten und aufzuzeichnen und dadurch die Netzwerkintegrität zu schützen und Sicherheitsverletzungen zu erkennen. Der Flow Sensor verfügt über integrierte webbasierte Managementsysteme, die Management und Administration sowohl zentralisiert als auch Remote vereinfachen.

Die Flow Sensor-Appliance ist am effektivsten, wenn sie wie folgt in kritischen Segmenten Ihres Unternehmensnetzwerks platziert wird:

- Innerhalb Ihrer Firewall, um den Datenverkehr zu überwachen und festzustellen, ob ein Firewall-Verstoß aufgetreten ist
- Außerhalb Ihrer Firewall, um den Netzwerkverkehr zu überwachen und zu analysieren, wer Ihre Firewall bedroht
- In sensiblen Bereichen Ihres Netzwerks, um Schutz vor verärgerten Mitarbeitern oder Hackern mit Root-Zugriff zu bieten
- An Remote-Standorten, die gefährdete Netzwerkerweiterungen darstellen
- In Ihrem Unternehmensnetzwerk, um die Protokollnutzung zu verwalten (z. B. in Ihrem Transaktionsservices-Subnetz, um festzustellen, ob ein Hacker Telnet oder FTP ausführt und die Finanzdaten Ihrer Kunden gefährdet)

Platzierung des Stealthwatch UDP Directors

Die einzige Voraussetzung für die Platzierung des Stealthwatch UDP Director ist, dass er über einen ungehinderten Kommunikationsweg zu den übrigen Stealthwatch-Appliances verfügt.

Konfigurieren Ihrer Firewall für die Kommunikation

Damit die Appliances richtig kommunizieren können, sollten Sie das Netzwerk so konfigurieren, dass Firewalls oder Zugriffskontrolllisten die erforderlichen Verbindungen nicht blockieren. Verwenden Sie dass Diagramm und die Tabellen in diesem Abschnitt, um Ihr Netzwerk so zu konfigurieren, dass die Appliances über das Netzwerk kommunizieren können.

Wenden Sie sich an Ihren Netzwerkadministrator, um sicherzustellen, dass die folgenden Ports offen sind und uneingeschränkten Zugriff haben:

- TCP 22
- TCP 25
- TCP 389

- TCP 443
- TCP 2393
- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Kommunikations-Ports

Die folgende Tabelle zeigt, wie die Ports in Stealthwatch verwendet werden:

Von (Client)	An (Server)	Port	Protokoll
Admin-Benutzer-PC	Alle Appliances	TCP/443	HTTPS
Alle Appliances	Netzwerk-Zeitquelle	UDP/123	NTP
Active Directory	Stealthwatch Management Console	TCP/389, UDP/389, UDP/389	LDAP
AnyConnect	Endpunkt Concentrator	UDP/2055	NetFlow
Cisco ISE	Stealthwatch Management Console	TCP/443	HTTPS
Cisco ISE	Stealthwatch Management Console	TCP/5222	XMPP
Endpunkt-Con-centrator	Flow Collector	UDP/2055	NetFlow
Externe Pro-tokollquellen	Stealthwatch Management Console	UDP/514	SYSLOG
Flow Collector	Stealthwatch Management Console	TCP/443	HTTPS
SLIC	Stealthwatch Management Console	TCP/443 oder Proxy-Ver-bindung	HTTPS
UDP Director	Flow Collector – sFlow	UDP/6343	sFlow
UDP Director	Flow Collector – NetFlow	UDP/2055*	NetFlow
UDP Director	Ereignismanagement-	UDP/514	SYSLOG

Von (Client)	An (Server)	Port	Protokoll
	Systeme von Drittanbietern		
Flow Sensor	Stealthwatch Management Console	TCP/443	HTTPS
Flow Sensor	Flow Collector – NetFlow	UDP/2055	NetFlow
Identität	Stealthwatch Management Console	TCP/2393	SSL
NetFlow-Exporter	Flow Collector – NetFlow	UDP/2055*	NetFlow
sFlow-Exporter	Flow Collector – sFlow	UDP/6343*	sFlow
Stealthwatch Management Console	Cisco ISE	TCP/443	HTTPS
Stealthwatch Management Console	DNS	UDP/53	DNS
Stealthwatch Management Console	Flow Collector	TCP/443	HTTPS
Stealthwatch Management Console	Flow Sensor	TCP/443	HTTPS
Stealthwatch Management Console	Identität	TCP/2393	SSL
Stealthwatch Management Console	Flow-Exporter	UDP/161	SNMP
Stealthwatch Management Console	Endpunkt-Concentrator	UDP.2055	HTTPS
Benutzer-PC	Stealthwatch Management Console	TCP/443	HTTPS

*Dies ist der Standardport, aber auf dem Exporter kann jeder UDP-Port konfiguriert werden.

Die folgende Tabelle gilt für optionale Konfigurationen, die durch die Anforderungen Ihres Netzwerks bestimmt werden:

Von (Client)	An (Server)	Port	Protokoll
Alle Appliances	Benutzer-PC	TCP/22	SSH
Stealthwatch Management Console	Ereignismanagement durch Drittanbieter	UDP/162	SNMP-Trap
Stealthwatch Management Console	Ereignismanagement durch Drittanbieter	UDP/514	SYSLOG
Stealthwatch Management Console	E-Mail-Gateway	TCP/25	SMTP
Stealthwatch Management Console	SLIC	TCP/443	SSL
Benutzer-PC	Alle Appliances	TCP/22	SSH

Das folgende Diagramm zeigt die verschiedenen Verbindungen, die von Stealthwatch verwendet werden. Die als optional gekennzeichneten Ports können entsprechend den Anforderungen Ihres eigenen Netzwerks verwendet werden.

Integration des Flow Sensors in Ihr Netzwerk

Der Stealthwatch Flow Sensor ist vielseitig einsetzbar und lässt sich in eine Vielzahl von Netzwerktopologien, -technologien und -komponenten integrieren. Es können zwar nicht alle Netzwerkkonfigurationen hier besprochen werden, die Beispiele helfen Ihnen jedoch möglicherweise, das beste Setup für Ihre Bedürfnisse zu finden.

Bevor Sie einen Flow Sensor installieren, müssen Sie mehrere Entscheidungen über Ihr Netzwerk und seine gewünschte Überwachung treffen. Analysieren Sie in jedem Fall sowohl die Topologie Ihres Netzwerks als auch Ihre spezifischen Überwachungsanforderungen. Es wird empfohlen, einen Flow Sensor so zu verbinden, dass er Netzwerkübertragungen zu und von dem überwachten Netzwerk und, falls gewünscht, auch interne Netzwerkübertragungen empfängt.

In den folgenden Abschnitten wird erläutert, wie Sie eine Stealthwatch Flow Sensor-Appliance mit den folgenden Ethernet-Netzwerkgeräten in Ihr Netzwerk integrieren können:

- **TAPs**
- **SPAN-Ports**

TAPs

Wenn ein Test Access Port (TAP) in Reihe mit einer Netzwerkverbindung platziert wird, sendet er die Signale der Verbindung an einem oder mehreren separaten Ports weiter. So sendet beispielsweise ein Ethernet-TAP, der in Reihe mit einem Ethernet-Kabel platziert ist, jede Übertragungen aus beiden Richtungen auf separaten Ports weiter. Daher ist die Verwendung eines TAP die zuverlässigste Art, den Flow Sensor zu verwenden. Welche Art von TAP Sie verwenden, hängt von Ihrem Netzwerk ab.

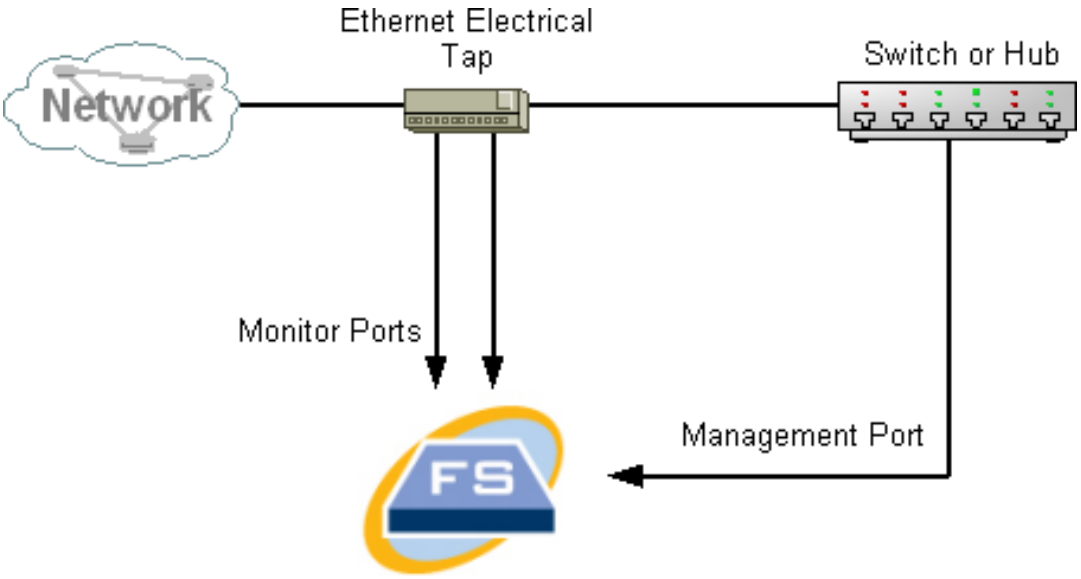
In diesem Abschnitt werden die folgenden Möglichkeiten zur Verwendung von TAPs erläutert:

- **Verwendung von elektrischen TAPs**
- **Verwendung von optischen TAPs**
- **Verwendung von TAPs außerhalb Ihrer Firewall**
- **Platzieren des Flow Sensors in Ihrer Firewall**

In einem Netzwerk mit TAPs kann der Flow Sensor nur dann Leistungsüberwachungsdaten erfassen, wenn er mit einem aggregierenden TAP verbunden ist, der sowohl eingehenden als auch ausgehenden Datenverkehr erfasst. Wenn der Flow Sensor an einen unidirektionalen TAP angeschlossen ist, der nur eine Datenverkehrsrichtung an jedem Port erfasst, erfasst der Flow Sensor keine Leistungsüberwachungsdaten.

Verwendung von elektrischen TAPs

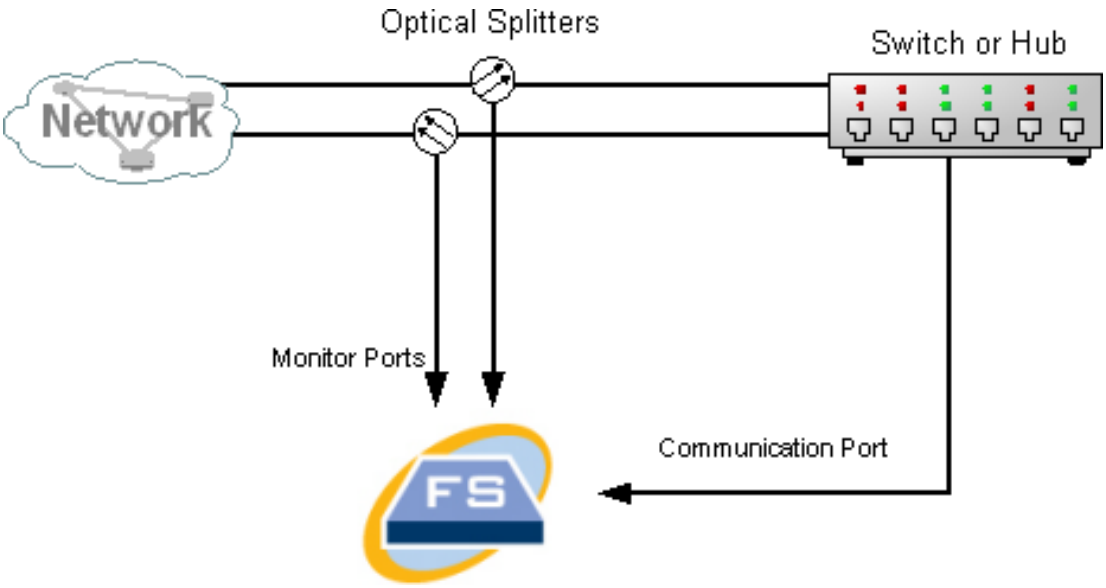
Im folgenden Beispiel ist der Flow Sensor an einen elektrischen Ethernet-TAP angeschlossen. Verbinden Sie dazu die beiden TAP-Ports mit den Monitor-Ports 1 und 2 des Flow Sensors.



Verwendung von optischen TAPs

Verwenden Sie zwei Splitter für faseroptische Systeme. Platzieren Sie einen Glasfaserkabelsplitter in Reihe mit jeder Übertragungsrichtung, um das optische Signal für eine Übertragungsrichtung weiterzusenden.

Im folgenden Beispiel ist der Flow Sensor an ein faseroptisches Netzwerk angeschlossen. Schließen Sie dazu die Ausgänge der Splitter an die Überwachungs-Ports 1 und 2 des Flow Sensors an.



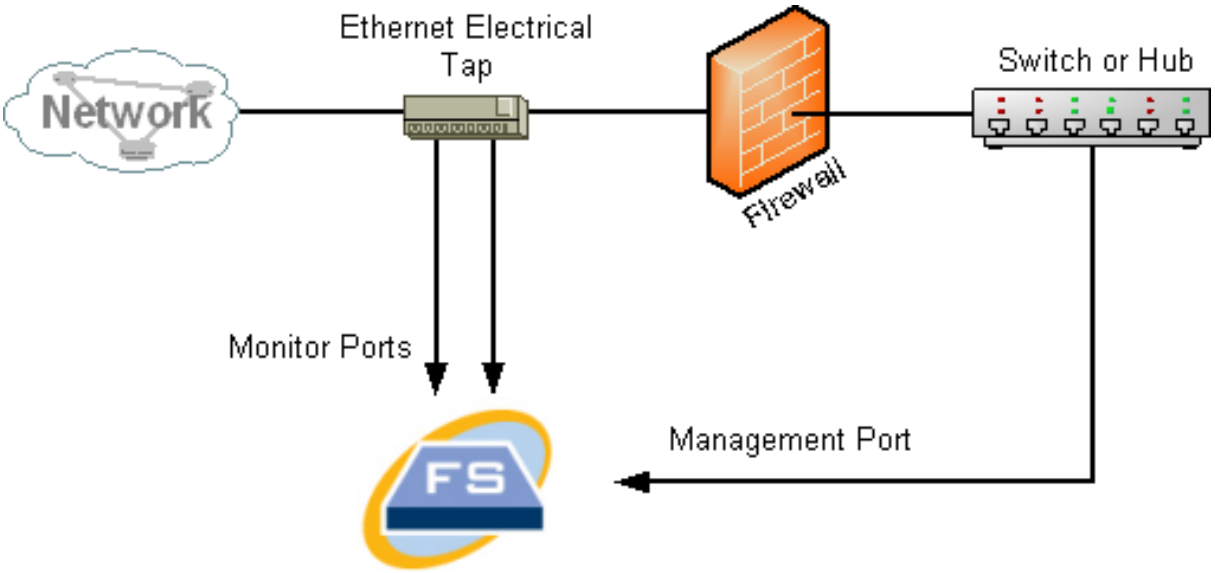
Wenn die Verbindung zwischen den überwachten Netzwerken eine optische Verbindung ist, wird der Flow Sensor mit zwei optischen Splittern verbunden. Der Management-Port ist entweder mit dem Switch des überwachten Netzwerks oder mit einem anderen Switch oder Hub verbunden.

Verwendung von TAPs außerhalb Ihrer Firewall

Damit der Flow Sensor den Datenverkehr zwischen Ihrer Firewall und anderen Netzwerken überwachen kann, verbinden Sie den Stealthwatch Management-Port mit einem Switch oder Port außerhalb der Firewall.

Wir empfehlen Ihnen dringend, für diese Verbindung einen TAP zu verwenden, damit durch einen Ausfall des Geräts nicht Ihr gesamtes Netzwerk ausfällt.

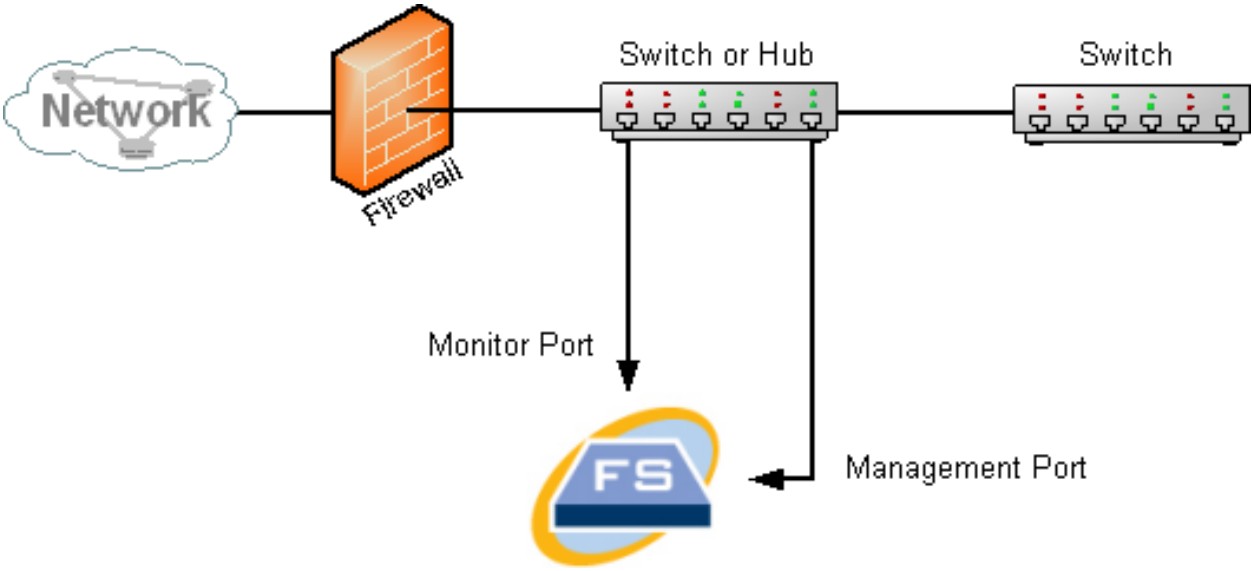
Im folgenden Beispiel ist die Verwendung eines elektrischen Ethernet-TAPs dargestellt. Der Management-Port muss mit dem Switch oder Hub des überwachten Netzwerks verbunden sein. Dieses Setup ähnelt demjenigen, das den Datenverkehr zu und von Ihrem Netzwerk überwacht.



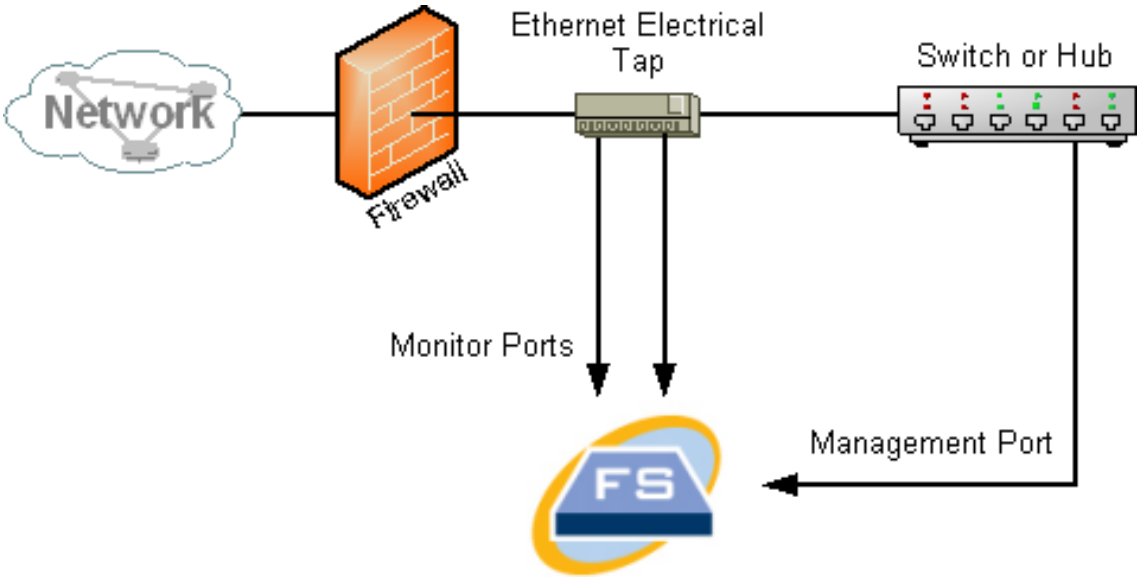
Wenn Ihre Firewall die Network Address Translation (NAT) durchführt, können Sie nur die Adressen beobachten, die sich auf der Firewall befinden.

Platzieren des Flow Sensors in Ihrer Firewall

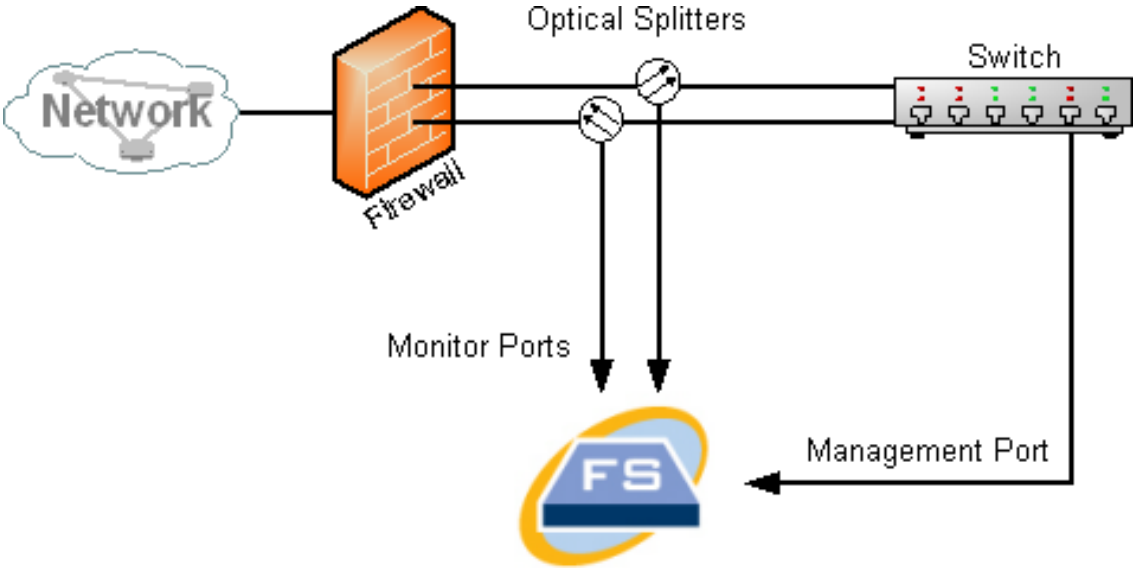
Um den Datenverkehr zwischen internen Netzwerken und einer Firewall zu überwachen, muss der Flow Sensor auf den gesamten Datenverkehr zwischen der Firewall und den internen Netzwerken zugreifen können. Dies können Sie erreichen, indem Sie einen Mirror-Port konfigurieren, der die Verbindung zur Firewall auf dem Haupt-Switch spiegelt. Stellen Sie sicher, dass Monitor-Port 1 des Flow Sensors mit dem Mirror-Port verbunden ist, wie in der folgenden Abbildung dargestellt:



Um den Datenverkehr innerhalb Ihrer Firewall mit Hilfe eines TAP zu überwachen, platzieren Sie den TAP oder den optischen Splitter zwischen Ihre Firewall und dem Haupt-Switch oder -Hub. Eine TAP-Konfiguration ist unten dargestellt..



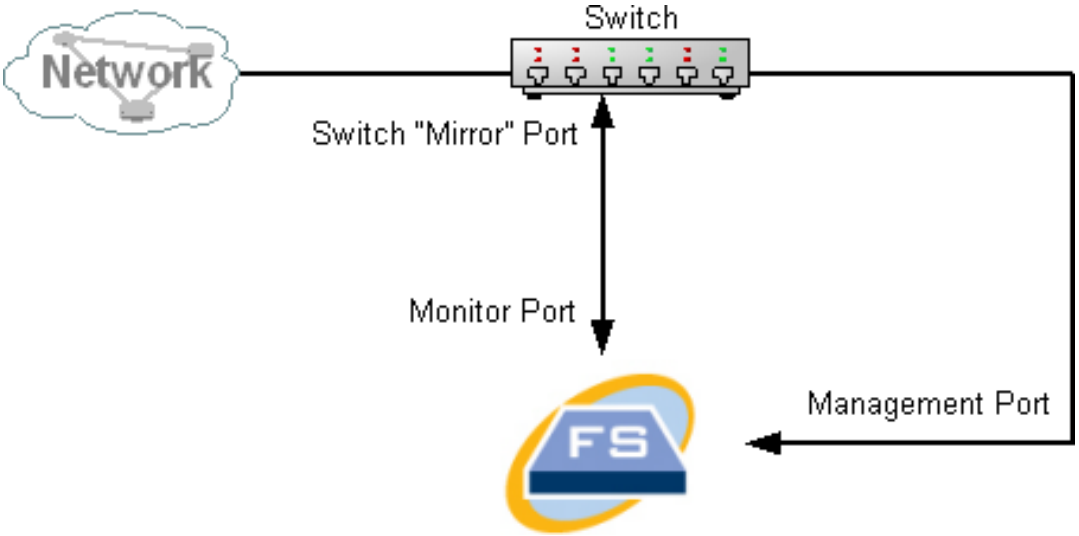
Eine Beispielkonfiguration des optischen Splitters ist unten dargestellt.



SPAN-Ports

Sie können den Flow Sensor auch an einen Switch anschließen. Da ein Switch jedoch nicht den gesamten Datenverkehr auf jedem Port weitersendet, wird der Flow Sensor nicht ordnungsgemäß funktionieren, es sei denn, der Switch kann Pakete weitersenden, die von und zu einem oder mehreren Switch-Ports gesendet werden. Diese Art von Switch-Port wird manchmal als Mirror-Port oder Switch Port Analyzer (SPAN) bezeichnet.

Die folgende Abbildung zeigt, wie Sie diese Konfiguration erreichen können, indem Sie Ihr Netzwerk über den Management-Port mit dem Stealthwatch Flow Sensor verbinden.



In dieser Konfiguration müssen Sie einen Switch-Port (auch Mirror-Port genannt) so konfigurieren, dass er den gesamten Datenverkehr vom und zum Host, der für den Mirror-Port von Interesse ist, weitersendet. Monitor-Port 1 des Flow Sensors muss mit diesem Mirror-Port verbunden sein. Dadurch kann der Flow Sensor den Datenverkehr zu und von dem betreffenden Netzwerk und zu anderen Netzwerken zu überwachen. In diesem Fall kann ein Netzwerk aus einigen oder allen mit dem Switch verbundenen Hosts bestehen.

Eine gängige Art, Netzwerke auf einem Switch zu konfigurieren, besteht darin, sie in Virtual Local Area Networks (VLANs) zu unterteilen, bei denen es sich um logische anstatt um physische Verbindungen von Hosts handelt. Wenn der Mirror-Port so konfiguriert ist, dass er alle Ports eines VLANs oder Switches spiegelt, kann der Flow Sensor den gesamten Datenverkehr zu, von und innerhalb des betreffenden Netzwerks sowie andere Netzwerke überwachen.

In allen Fällen empfehlen wir Ihnen, die Dokumentation Ihres Switch-Herstellers zu lesen, um festzustellen, wie Sie den Mirror-Port des Switches konfigurieren und welcher Datenverkehr zum Mirror-Port weitergesendet wird.

Installation

In diesem Abschnitt wird die Installation Ihrer Appliances in Ihrer Umgebung beschrieben. Enthalten sind:

- **Montage Ihrer Appliance**
- **Verbinden Ihrer Appliance mit dem Netzwerk**
- **Verbinden mit Ihrer Appliance**
- **Ändern von Standardinformationen**

Montage Ihrer Appliance

Sie können Stealthwatch-Appliances direkt in einem Standard-19"-Rack oder -Schrank, einem anderen geeigneten Schrank oder auf einer ebenen Fläche montieren. Wenn Sie eine Appliance in einem Rack oder Schrank montieren, befolgen Sie die Anweisungen zu den Gleitschienen-Sätzen. Bei der Bestimmung des Aufstellungsortes einer Appliance ist auf folgenden Abstand zur Vorder- und Rückseite zu achten:

- Die Anzeigen auf der Vorderseite sind gut ablesbar
- Der Zugang zu den Ports an der Rückseite ist für eine problemlose Verkabelung ausreichend
- Der Netzanschluss an der Rückseite befindet sich in Reichweite einer konditionierten Wechselstromquelle.
- Der Luftstrom rund um die Appliance und durch die Lüfter ist unbeschränkt.

Im Lieferumfang der Appliance enthaltene Hardware

Die folgende Hardware ist im Lieferumfang der Stealthwatch-Appliances enthalten:

- Wechselstromkabel
- Zugangsschlüssel (für Frontplatte)
- Gleitschienen-Satz für die Rackmontage oder Montagelaschen für kleinere Appliances
- Für den Flow Collector 5210 ist ein 10-GB-SFP-Kabel erforderlich

Zusätzlich erforderliche Hardware

Sie müssen die folgende zusätzlich erforderliche Hardware bereitstellen:

- Befestigungsschraube für ein Standard-19“-Rack
- Unterbrechungsfreie Stromversorgung (USV) für jede Appliance, die Sie installieren
- Um lokal zu konfigurieren (optional), verwenden Sie eine der folgenden Methoden:
  - Laptop mit einem Videokabel und einem USB-Kabel (für die Tastatur)
  - Videomonitor mit einem Videokabel und Tastatur mit einem USB-Kabel

Verbinden Ihrer Appliance mit dem Netzwerk

Verwenden Sie das gleiche Verfahren, um jede Appliance mit dem Netzwerk zu verbinden. Der einzige Unterschied für den Anschluss ist die Art von Appliance, die Sie haben.

Detaillierte Informationen zu den einzelnen Appliances finden Sie in den Stealthwatch-Datenblättern.

> Alle Hardwarekomponenten der Cisco x210-Serie verwenden die gleiche UCS-Plattform, UCSC-C220-M5SX. Die einzige Ausnahme ist der Flow Collector 5210 DB, der UCSC-C240-M5SX verwendet. Die Unterschiede in den Appliances liegen bei NIC-Karten, Prozessor, Arbeitsspeicher, Speicher und RAID.

> Der Flow Collector 5210 besteht aus zwei miteinander verbundenen Servern (Engine und Datenbank), so dass sie wie eine einzige Appliance funktionieren. Dadurch unterscheidet sich die Installation leicht vom Verfahren bei anderen Appliances. Verbinden Sie sie zunächst direkt über ein 10G-SFP+-DA-Cross-Connect-Kabel. Stellen Sie anschließend eine Verbindung mit Ihrem Netzwerk her.

So verbinden Sie Ihre Appliance mit Ihrem Netzwerk:

1. Schließen Sie ein Ethernet-Kabel an den Management-Port auf der Rückseite der Appliance an.
2. Schließen Sie mindestens einen Überwachungs-Port für Flow Sensoren und UDP Directors an.

   Verbinden Sie beim UDP Director HA die beiden UDP Directors durch Crossover-Kabel. Verbinden Sie den eth2-Port eines UDP Directors mit dem eth2-Port des zweiten UDP Directors. Verbinden Sie ebenfalls den eth3-Port jedes UDP-Directors mit einem zweiten Crossover-Kabel. Das Kabel kann aus Glasfaser oder

Kupfer sein.

Notieren Sie unbedingt das Ethernet-Label (eth2, eth3 usw.) für jeden Port. Diese Bezeichnungen entsprechen den Netzwerkschnittstellen (eth2, eth3 usw.), die auf der Startseite der Verwaltungsoberfläche der Appliance angezeigt und konfiguriert werden können.

3. Verbinden Sie das jeweils andere Ende der Ethernet-Kabel mit dem Switch Ihres Netzwerks.
4. Verbinden Sie die Netzkabel mit dem Netzteil. Einige Appliances verfügen über zwei Stromanschlüsse: Netzteil 1 und Netzteil 2.

Verbinden mit Ihrer Appliance

In diesem Abschnitt wird beschrieben, wie Sie sich mit Ihrer Appliance verbinden, um die Standard-Benutzerkennwörter zu ändern.

Sie können sich auf zwei Arten mit der Appliance verbinden:

- mit Tastatur und Monitor
- mit einem Laptop (und einem Terminal-Emulator)

Bei neuen Appliances ist SSH deaktiviert. Sie müssen sich bei der Weboberfläche „Administration“ der Appliance anmelden, um es zu aktivieren.

Anschluss einer Tastatur und eines Monitors

Gehen Sie wie folgt vor, um die IP-Adresse lokal zu konfigurieren:

1. Stecken Sie das Netzkabel in die Appliance.
2. Drücken Sie den Netzschalter, um die Appliance Gerät einzuschalten. Warten Sie, bis der Boot-Vorgang abgeschlossen ist. Unterbrechen Sie den Boot-Vorgang nicht.

> Möglicherweise müssen Sie die Frontplatte entfernen, um die Stromversorgung herzustellen.
>
> Bei einigen Modellen schalten sich die Lüfter der Stromversorgung ein, während das System nicht eingeschaltet ist. Überprüfen Sie, ob die LED auf der Frontplatte leuchtet.
>
> Achten Sie darauf, die Appliance an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Das Netzteil benötigt Strom; andernfalls zeigt das System einen Fehler an.

3. Schließen Sie die Tastatur an:

- Wenn Sie eine Standardtastatur haben, schließen Sie sie an den Standard-Tastaturanschluss an.
- Wenn Sie eine USB-Tastatur besitzen, schließen Sie diese an einen USB-Anschluss an.

4. Schließen Sie das Videokabel an den Videoanschluss an. Die Anmeldeaufforderung wird angezeigt.

5. Fahren Sie fort mit dem Abschnitt **Ändern von Standardinformationen**.

Verbindung mit einem Laptop herstellen

Sie können die Appliance auch mit einem Laptop mit Terminal-Emulator verbinden.

So verbinden Sie eine Appliance mit einem Laptop:

1. Schließen Sie Ihren Laptop mit einer der folgenden Methoden an die Appliance an:
   - Schließen Sie ein RS232-Kabel vom seriellen Port (DB9) Ihres Laptops an den Konsolen-Port der Appliance an.
   - Verbinden Sie ein Crossover-Kabel vom Ethernet-Port Ihres Laptops mit dem Management-Port der Appliance.
2. Stecken Sie das Netzkabel in die Appliance.
3. Drücken Sie den Netzschalter, um die Appliance Gerät einzuschalten. Warten Sie, bis der Boot-Vorgang abgeschlossen ist. Unterbrechen Sie den Boot-Vorgang nicht.

   > Möglicherweise müssen Sie die Frontplatte entfernen, um die Stromversorgung herzustellen.
   >
   > Bei einigen Modellen schalten sich die Lüfter der Stromversorgung ein, während das System nicht eingeschaltet ist. Überprüfen Sie, ob die LED auf der Frontplatte leuchtet. Achten Sie darauf, die Appliance an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Das Netzteil benötigt Strom; andernfalls zeigt das System einen Fehler an.

4. Stellen Sie auf dem Laptop eine Verbindung zur Appliance her.

   Sie können jeden verfügbaren Terminal-Emulator verwenden, um mit der Appliance zu kommunizieren.

5. Übernehmen Sie die folgenden Einstellungen:
   - BPS: 115200
   - Datenbits: 8
   - Stoppbit: 1
   - Parität: Keine
   - Flusskontrolle: keine

   Der Anmeldebildschirm und die Anmeldeaufforderung werden angezeigt.

6. Fahren Sie fort mit dem nächsten Abschnitt, **Ändern von Standardinformationen**.

Ändern von Standardinformationen

Nachdem Sie sich mit der Appliance verbunden haben, konfigurieren Sie die IP-Adressen und ändern Sie die Benutzerkennwörter.

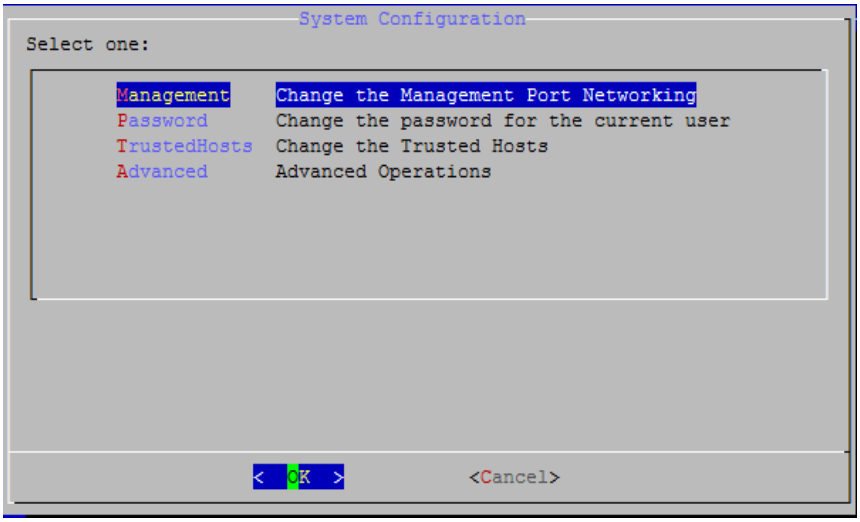
Ändern der Standard-IP-Adressen

Die Appliances haben bereits Standard IP-Adressen. Sie können diese jedoch für Ihr Netzwerk konfigurieren.

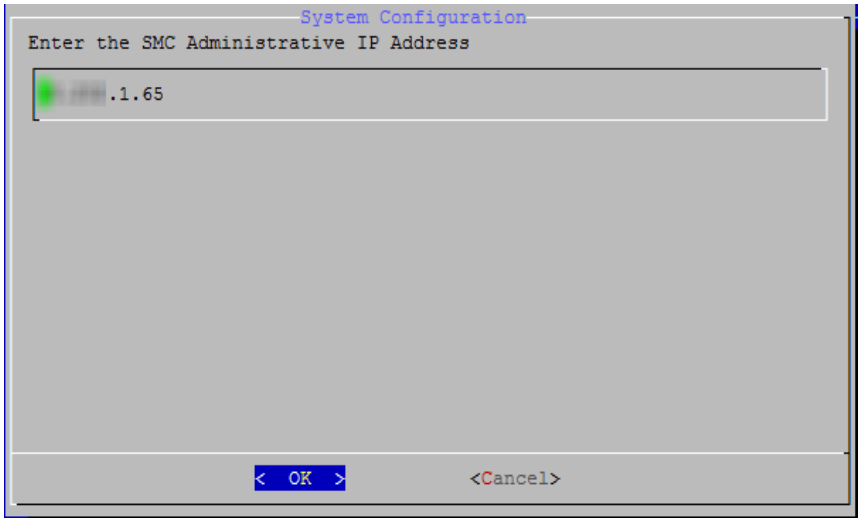
1. Melden Sie sich beim Programm „Systemkonfiguration“ an:

   - Geben Sie **sysadmin** ein und drücken Sie die **Eingabetaste**.
   - Wenn die Kennwortabfrage erscheint, geben Sie **lan1cope** ein und drücken Sie dann die **Eingabetaste**.
   - Geben Sie bei der nächsten Eingabeaufforderung **SystemConfig** ein und drücken Sie dann die **Eingabetaste**.

     Das Menü „Systemkonfiguration“ wird geöffnet.

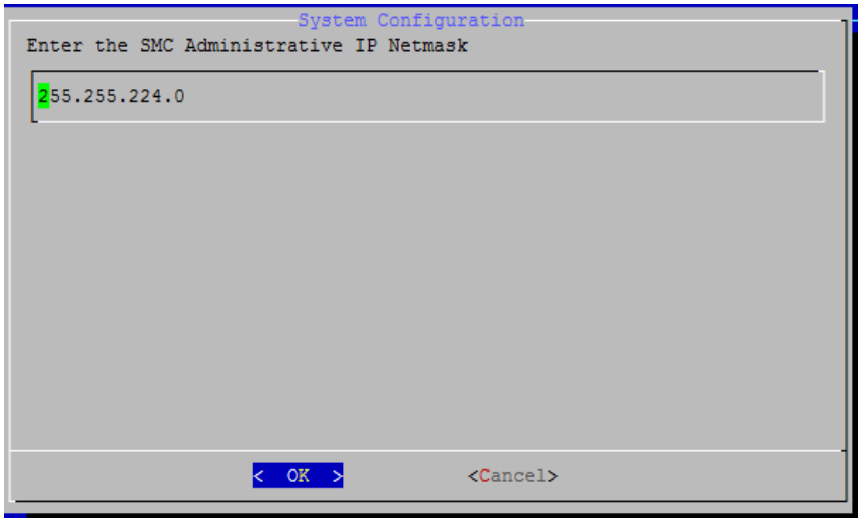


2. Wählen Sie **Management** und drücken Sie dann die **Eingabetaste**. Die Seite „IP-Adresse“ wird geöffnet.



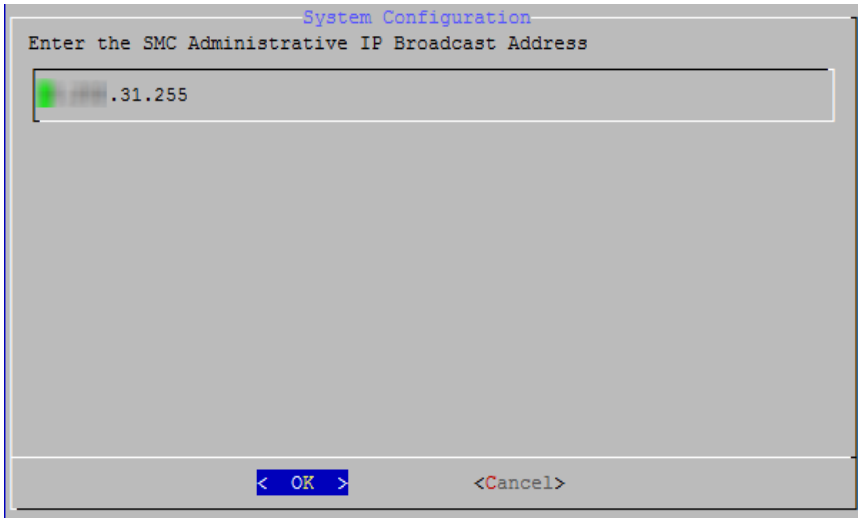
3. Geben Sie eine neue IP-Adresse basierend auf Ihrer Umgebung ein. Wählen Sie **OK** und drücken Sie dann die **Eingabetaste**, um fortzufahren.

   Die IP-Netzmaskenseite wird mit dem Standardwert geöffnet.



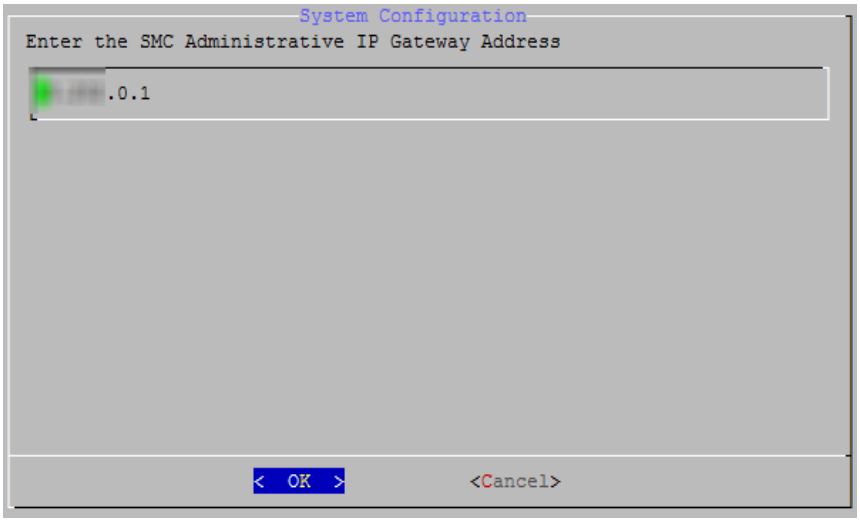
4. Übernehmen Sie den Standardwert oder geben Sie eine neue IP-Netzmaskenadresse basierend auf Ihrer Umgebung ein. Wählen Sie **OK,** und drücken Sie dann die **Eingabetaste**, um fortzufahren.

Die Seite „Broadcast-Adresse“ wird geöffnet.



5. Übernehmen Sie den Standardwert oder geben Sie einen neuen ein, der auf Ihrer Umgebung basiert. Wählen Sie **OK** und drücken Sie dann die **Eingabetaste**, um fortzufahren.

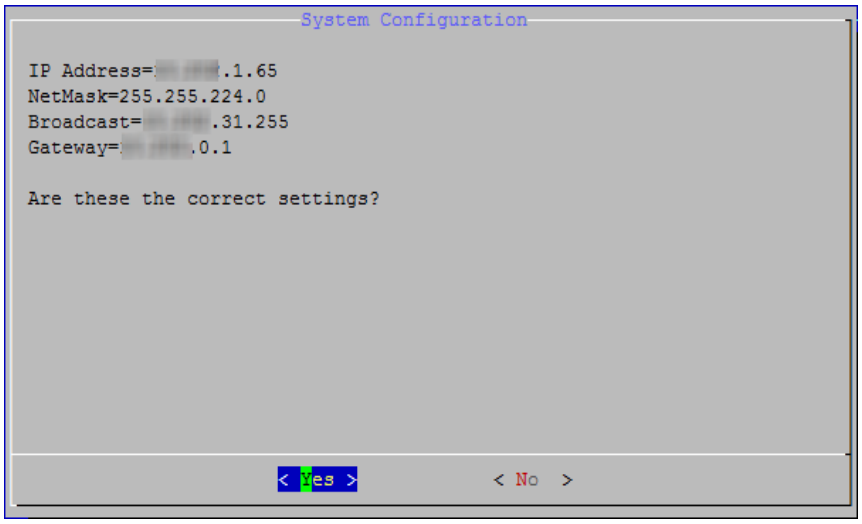
   Die Seite „Gateway-Adresse“ wird mit der standardmäßigen IP-Adresse des Gateway-Servers geöffnet.



6. Übernehmen Sie den Standardwert oder geben Sie einen neuen ein, der auf Ihrer Umgebung basiert. Wählen Sie **OK** und drücken Sie dann die **Eingabetaste**, um

fortzufahren.

Die Bestätigungsseite wird geöffnet.



7. Überprüfen Sie die Informationen. Sind die Einstellungen korrekt?

- Wenn ja, wählen Sie **Ja,** und drücken Sie dann die **Eingabetaste**, um fortzufahren. Das System startet neu und übernimmt die Änderungen. Nach Abschluss öffnet sich die Anmmeldeseite.
- Wenn nicht, wählen Sie **Nein**, um Korrekturen vorzunehmen. Die Seite „IP-Adresse“ wird geöffnet, damit Sie Ihre Änderungen vornehmen können. Nachdem die Änderungen vorgenommen wurden und Sie die Einstellungen übernommen haben, öffnet sich die Seite „Neustart“. Drücken Sie die **Eingabetaste**, um Ihre Änderungen zu übernehmen.***Es wurde keine Neustart-Meldungsseite angezeigt.***

8. Fahren Sie fort mit dem nächsten Abschnitt,**Ändern des Sysadmin-Benutzerkennworts**.

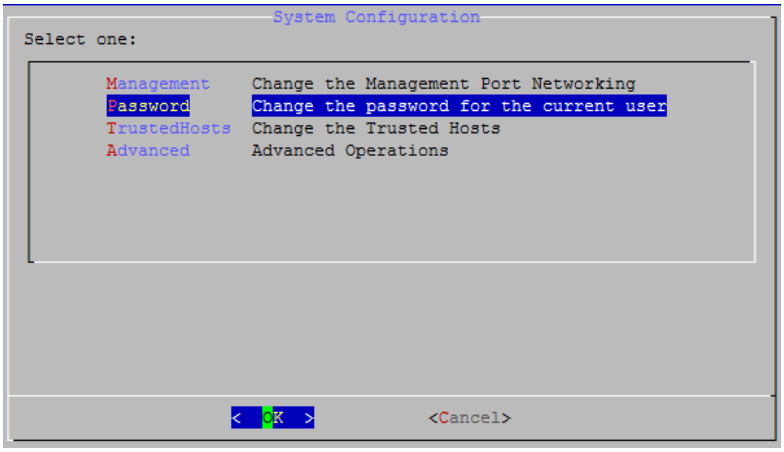
Ändern des Sysadmin-Benutzerkennworts

Um die Sicherheit Ihres Netzwerks zu gewährleisten, ändern Sie das Standard-Sysadmin-Kennwort für Appliances.

Vergewissern Sie sich, dass Sie sich als **Sysadmin** angemeldet haben, um diesen Vorgang zu starten.

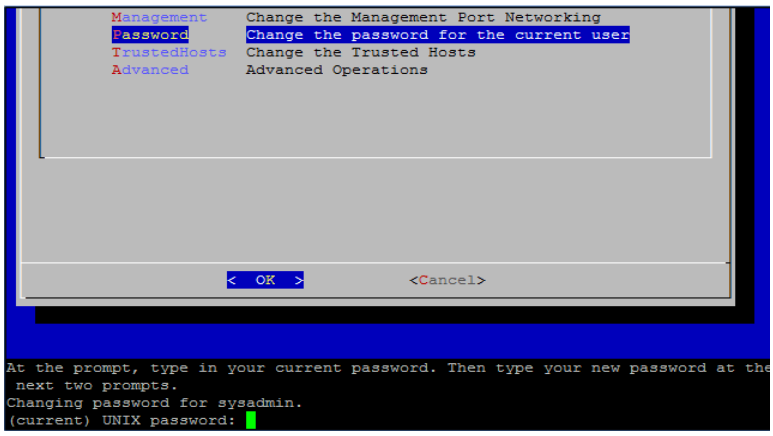
So ändern Sie das Sysadmin-Kennwort:

1. Wählen Sie im Menü „Systemkonfiguration“ **Kennwort** und drücken Sie die **Eingabetaste**.



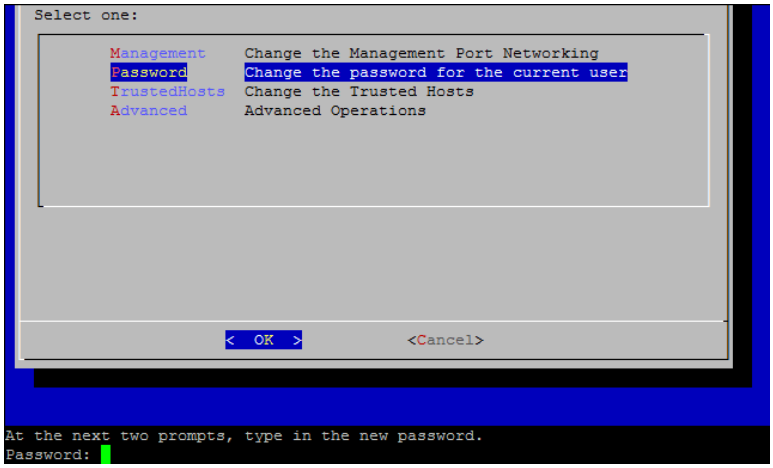
   Wenn Sie in den Standardeinstellungen die Liste der vertrauenswürdigen Hosts ändern, stellen Sie sicher, dass jede Stealthwatch-Appliance in der Liste der vertrauenswürdigen Hosts für jede andere Stealthwatch-Appliance in Ihrer Bereitstellung enthalten ist. Andernfalls können die Appliances nicht miteinander kommunizieren.

   Unterhalb des Menüs erscheint eine Eingabeaufforderung für das aktuelle Kennwort.



2. Geben Sie das aktuelle Kennwort ein und drücken Sie dann die **Eingabetaste**.

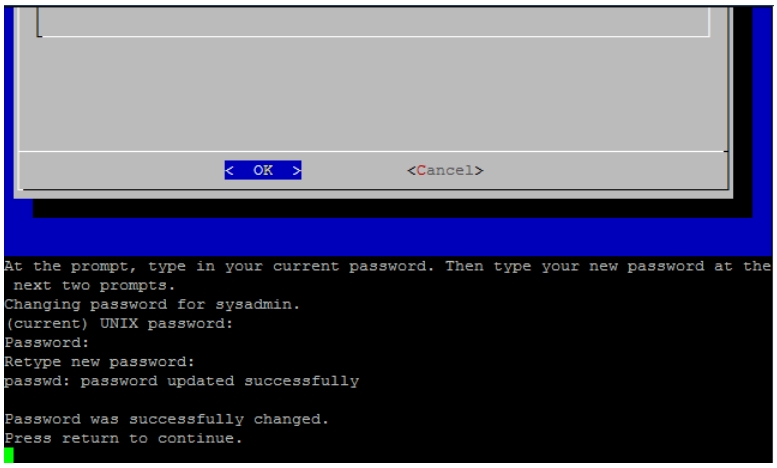
   Die Aufforderung zur Eingabe eines neuen Kennworts wird angezeigt.



3. Geben Sie das neue Kennwort ein und drücken Sie dann die **Eingabetaste**.

   Das Kennwort muss zwischen 8 und 30 alphanumerische Zeichen lang sein und darf keine Leerzeichen enthalten. Außerdem können Sie folgende Sonderzeichen verwenden: $.~!@#%_=?:,{}()

4. Geben Sie das Kennwort erneut ein und drücken Sie dann die **Eingabetaste**.

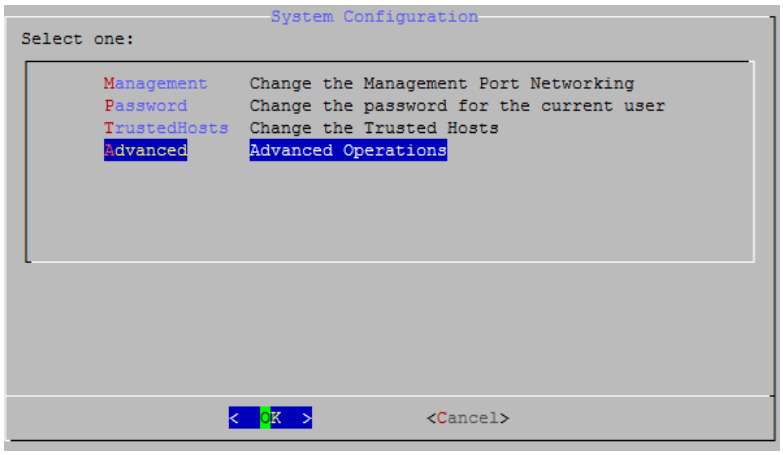


5. Wenn Ihr Kennwort akzeptiert wird, drücken Sie erneut die **Eingabetaste**, um zum Menü „Systemkonfiguration“ zurückzukehren.
6. Fahren Sie fort mit dem nächsten Abschnitt, **Ändern des Root-Benutzerkennworts**

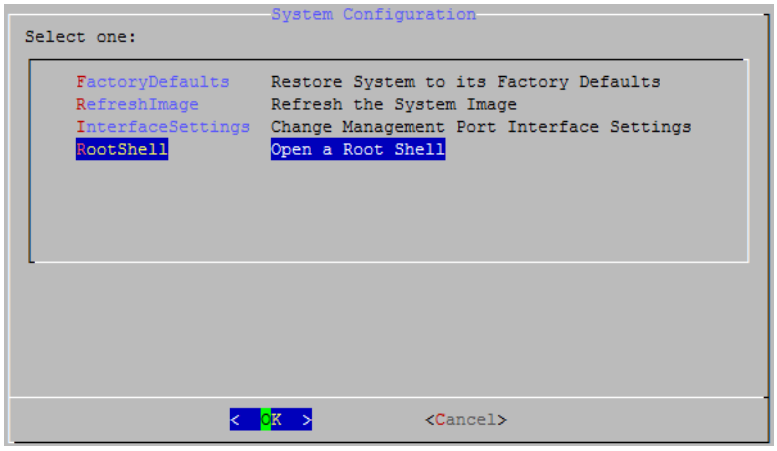
Ändern des Root-Benutzerkennworts

Nachdem Sie das Standard-Sysadmin-Benutzerkennwort geändert haben, ändern Sie das Standard-Root-Benutzerkennwort, um die Sicherheit Ihres Netzwerks zusätzlich zu schützen.

1. Navigieren Sie zur Root-Shell.

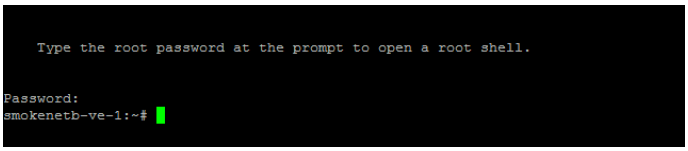


2. Wählen Sie im Menü „Systemkonfiguration“ **Erweitert** und drücken Sie dann die **Eingabetaste**. Das Menü „Erweitert“ wird angezeigt.

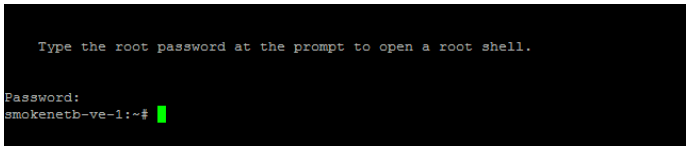


3. Wählen Sie **RootShell** und drücken Sie dann die **Eingabetaste**.

   Es erscheint eine Eingabeaufforderung für das Root-Kennwort.



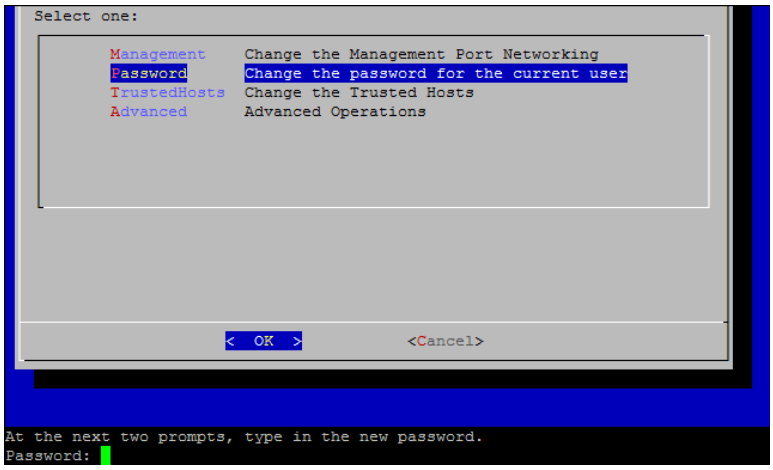
4. Geben Sie das aktuelle Root-Kennwort ein, und drücken Sie dann die **Eingabetaste**. Die Eingabeaufforderung für die Root-Shell wird angezeigt.



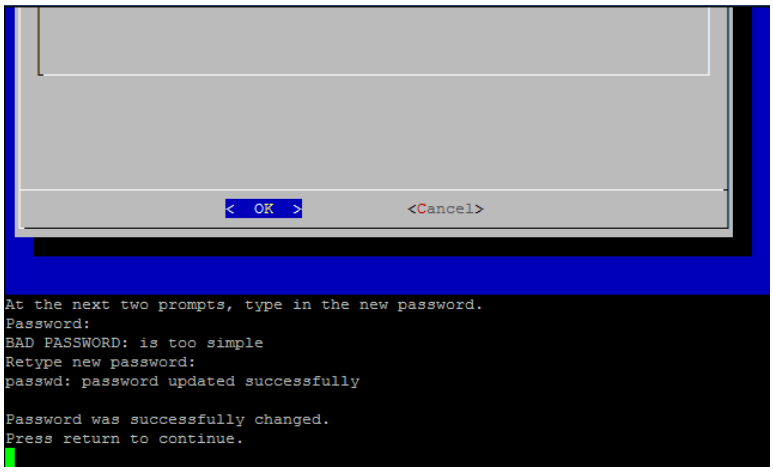
5. Geben Sie **SystemConfig** ein und drücken Sie die **Eingabetaste**.

   Dadurch kehren Sie zum Menü „Systemkonfiguration“ zurück, damit Sie das Root-Kennwort ändern können.

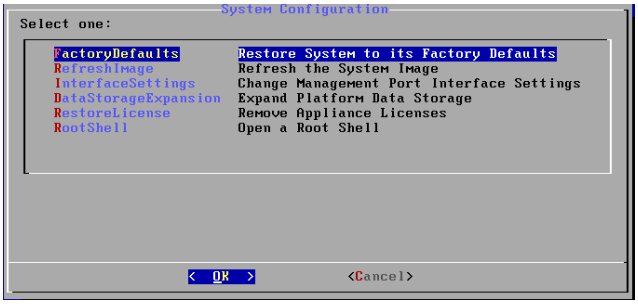
6. Wählen Sie **Kennwort** und drücken Sie dann die **Eingabetaste**. Die Kennwortabfrage erscheint unterhalb des Menüs.



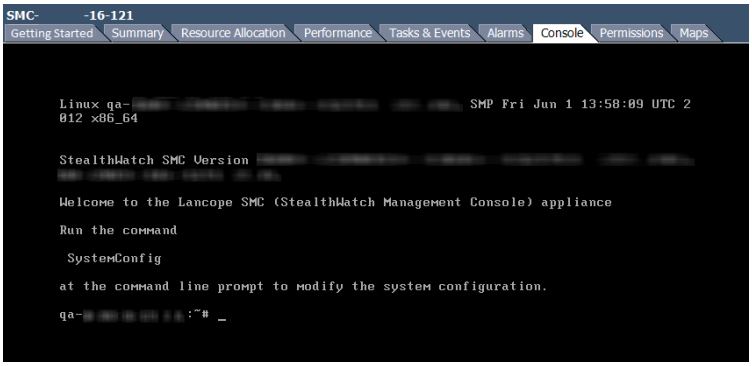
7. Geben Sie das neue Root-Kennwort ein und drücken Sie dann die **Eingabetaste**. Es erscheint eine zweite Eingabeaufforderung.



8. Geben Sie das neue Root-Kennwort erneut ein und drücken Sie dann die **Eingabetaste**.
9. Wenn Ihre Kennwortänderung erfolgreich war, drücken Sie die **Eingabetaste**. Sie haben nun sowohl Ihr Standard-Sysadmin- als auch Ihr Root-Kennwort geändert. Dadurch kehren Sie zum Konsolenmenü „Systemkonfiguration“ zurück.



10. Wählen Sie **Abbrechen** und drücken Sie die **Eingabetaste**. Die Konsole „Systemkonfiguration“ wird geschlossen und die Root-Shell-Eingabeaufforderung wird angezeigt.



11. Geben Sie **exit** ein und drücken Sie die **Eingabetaste**. Die Anmeldeaufforderung wird angezeigt.
12. Drücken Sie **Strg+Alt**, um die Konsolenumgebung zu verlassen.

Konfigurieren Ihrer Appliance

Sie sind nun bereit, Ihre Appliance zu konfigurieren. Informationen zur Konfiguration Ihrer Appliance finden Sie im entsprechenden **Stealthwatch-Handbuch für die Installation und Konfiguration** für Ihre Softwareversion. Die Serie x210 ist kompatibel mit den Stealthwatch-Softwareversionen 7.x.

Copyright Information