



Cisco Secure Network Analytics

Hardware-Appliance-Installationshandbuch für die x2xx-Serie 7.5.0



Inhalt

Einführung	5
Übersicht	5
Zielgruppe	6
Installieren von Appliances und Konfigurieren des Systems	6
Zugehörige Informationen	6
Terminologie	7
Häufige Abkürzungen	7
Informationen über Secure Network Analytics-Appliances	8
Manager 2210	8
Data Store 6200	8
Flow Collector 4210 und 5210	9
UDP Director 2210	9
Flow Sensor 1210, 3210 und 4240	10
Secure Network Analytics ohne Data Store	11
Secure Network Analytics mit Data Store	12
Abfragen	13
Data Store-Speicherung und Fehlertoleranz	13
Beispiel für Telemetriespeicher	14
Allgemeine Bereitstellungsanforderungen	15
Installationsmethoden	15
Kompatibilität	16
Allgemeine Anforderungen für alle Appliances	16
VMware	17
KVM	17
Software herunterladen	18
TLS	18
Anwendungen von Drittanbietern	18
Browser	18

Hostname	18
Domänenname	18
NTP-Server	19
Zeitzone	19
Standard-Appliance-Anforderungen (ohne Data Store)	19
Manager- und Flow Collector-Bereitstellungsanforderungen	19
Data Store-Bereitstellungsanforderungen	20
Appliance-Anforderungen (mit Data Store)	20
Manager- und Flow Collector-Bereitstellungsanforderungen	20
Data Node-Bereitstellungsanforderungen	21
Bereitstellung mehrerer Data Nodes	21
Unterstützte Hardwaremetriken (mit aktivierter Analytik)	22
Unterstützte Hardwaremetriken (ohne aktivierte Analytik)	22
Bereitstellung einzelner Data Nodes	22
Data Node-Konfigurationsanforderungen	23
Überlegungen zu Netzwerk und Switching	24
Hardware-Switch – Beispiel	26
Überlegungen zur Data Store-Platzierung	27
Die Analytik der Bereitstellungsanforderungen	28
1. Konfigurieren Ihrer Firewall für die Kommunikation	29
Offene Ports (alle Appliances)	29
Zusätzliche offene Ports für Data Nodes	29
Kommunikations -Ports und Protokolle	30
Zusätzliche offene Ports für Data Store	32
Optionale Kommunikations-Ports	34
Secure Network Analytics Bereitstellungsbeispiel	35
Secure Network Analytics Beispiel für eine Bereitstellung mit Data Store	36
2. Installationswarnungen und Richtlinien	37
Installationswarnungen	37
Installationsrichtlinien	44

Sicherheitshinweise	45
Sicherheit bei Arbeiten mit Elektrizität	46
Vermeidung von Schäden durch ESD	47
Standortumgebung	47
Überlegungen zur Stromversorgung	47
Überlegungen zur Rack-Konfiguration	48
3. Montage Ihrer Appliances	49
Im Lieferumfang der Appliance enthaltene Hardware	49
Zusätzlich erforderliche Hardware	49
4. Verbinden Ihrer Appliances mit dem Netzwerk	50
1. Spezifikationen prüfen	50
2. Verbinden Ihrer Appliance mit dem Netzwerk	51
5. Verbinden mit Ihrer Appliance	52
Anschluss einer Tastatur und eines Monitors	52
Anschluss eines seriellen Kabels oder einer seriellen Konsole	53
Verbinden mit CIMC (für Remote-Zugriff erforderlich)	54
6. Konfigurieren des Secure Network Analytics-Systems	55
Systemkonfigurationsanforderungen	55
Support kontaktieren	59
Änderungsverlauf	60

Einführung

Übersicht

Dieses Handbuch erklärt die Installation Cisco Secure Network Analytics der Hardware-Appliances der x2xx-Serie (ehemals Stealthwatch). Diese Anleitung beschreibt auch die Montage und Installation der Secure Network Analytics-Hardware.



Lesen Sie das Dokument [Erfüllung gesetzlicher Auflagen und Sicherheitsinformationen](#), bevor Sie Appliances der Secure Network Analytics x2xx-Serie installieren.

Die Hardware der x2xx-Serie umfasst:

Appliance	Teilenummer
Manager 2210 (ehemals Stealthwatch Management Console)	ST-SMC2210-K9
Data Store 6200 (drei Data Nodes)	ST-DS6200-K9 (drei ST-DNODE-G1)
Flow Collector 4210	ST-FC4210-K9
Flow Collector 5210 Engine	ST-FC5210-E
Flow Collector 5210-Datenbank	ST-FC5210-D
UDP Director 2210	ST-UDP2210-K9
Flow Sensor 1210	ST-FS1210-K9
Flow Sensor 3210	ST-FS3210-K9
Flow Sensor 4240	ST-FS4240-K9

Zielgruppe

Dieses Handbuch richtet sich an die Person, die für die Installation der Secure Network Analytics-Hardware verantwortlich ist. Wir gehen davon aus, dass Sie bereits über Grundkenntnisse in der Installation von Netzwerkgeräten verfügen.

Wenn Sie es vorziehen, mit einem unserer Installationsfachleute zusammenzuarbeiten, wenden Sie sich bitte an Ihren Cisco Partner vor Ort oder an den [Cisco Support](#).

Installieren von Appliances und Konfigurieren des Systems

Beachten Sie den allgemeinen Workflow für die Installation und Konfiguration von Secure Network Analytics.

1. **Installation von Appliances:** Installieren Sie mithilfe dieses Installationshandbuchs Ihre (physischen) Hardware-Appliances der Secure Network Analytics x2xx-Serie. Um Appliances der Virtual Edition zu installieren, befolgen Sie die Anweisungen im [Installationshandbuch für Appliances der Virtual Edition](#).
2. **Konfiguration Secure Network Analytics:** Nachdem Sie Hardware- und virtuelle Appliances installiert haben, können Sie Secure Network Analytics in einem gemanagten System konfigurieren. Befolgen Sie die Anweisungen aus dem [Secure Network Analytics-Systemkonfigurationshandbuch v7.5.0](#).

Zugehörige Informationen

Weitere Informationen zu Secure Network Analytics finden Sie in den folgenden Online-Ressourcen:

- **Erfüllung gesetzlicher Auflagen und Sicherheitsinformationen:** Lesen Sie das Dokument [Erfüllung gesetzlicher Auflagen und Sicherheitsinformationen](#), bevor Sie Appliances der Secure Network Analytics x2xx-Serie installieren.
- **Überblick:**
<https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>
- **Data Store-Designleitfaden:**
<https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf>
- **Hardware- und Softwareversionsmatrix:**
<https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html>
- **Appliance-Spezifikationen:**
<https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html>

Terminologie

In diesem Handbuch wird für jedes Secure Network Analytics-Produkt der Begriff **„Appliance“** verwendet.

Ein **„Cluster“** ist eine Gruppe von Secure Network Analytics-Appliances, die vom Manager verwaltet werden.

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	Switch Port Analyzer
TAP	Test Access Port
USV	Unterbrechungsfreie Stromversorgung
VLAN	Virtual Local Area Network

Informationen über Secure Network Analytics-Appliances

Secure Network Analytics 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 Secure Network Analytics x2xx-Serie.

Manager 2210

Der Manager verwaltet, koordiniert, konfiguriert und organisiert alle Einzelkomponenten des Systems. Mithilfe der Secure Network Analytics-Software können Sie über jeden Computer mit Webbrowser auf die Weboberfläche der Konsole zugreifen. Sie können problemlos auf Echtzeit-Sicherheits- und Netzwerkinformationen über kritische Segmente in Ihrem gesamten Unternehmen zugreifen. Mit der Java-basierten Plattformunabhängigkeit ermöglicht der Manager Folgendes:

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

Wenn Sie einen Data Store bereitstellen, können Sie einen Manager 2210 mit einer 10-Gbit/s-SFP+-DAC-Schnittstelle als eth0 für erhöhten Durchsatz konfigurieren. Wenn Sie keinen Data Store einsetzen, können Sie nur die 1-Gbit/s-/10-Gbit/s-Schnittstelle als eth0 konfigurieren.

Data Store 6200

Der Data Store bietet ein zentrales Repository zum Speichern der Telemetriedaten Ihres Netzwerks, die vom Flow Collector erfasst werden. Der Data Store besteht aus einem Cluster von Data Nodes, die jeweils einen Teil Ihrer Daten enthalten, und einem Backup von Daten eines separaten Data Node. Da sich alle Ihre Daten in einer zentralen Datenbank befinden und nicht über mehrere Flow Collectors verteilt sind, kann der Manager Abfrageergebnisse vom Data Store schneller abrufen, als wenn alle Flow Collectors separat abgefragt würden. Der Data Store-Cluster bietet eine verbesserte

Fehlertoleranz, eine verbesserte Antwort auf Abfragen und eine schnellere grafische Darstellung.

Weitere Informationen finden Sie unter [Secure Network Analytics mit Data Store](#).

Flow Collector 4210 und 5210

Der Flow Collector sammelt NetFlow-, cFlow-, J-Flow-, Packeteer2-, NetStream- und IPFIX-Daten, um einen verhaltensbasierten Netzwerkschutz zu bieten.

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

Wenn Sie einen Data Store bereitstellen, können Sie einen Flow Collector 4210 mit einer 10-Gbit/s- SFP+-DAC-Schnittstelle als eth0 für erhöhten Durchsatz konfigurieren. Wenn Sie keinen Data Store einsetzen, können Sie nur die 100-Mbit/s-/1-Gbit/s-/10-Gbit/s-Kupferschnittstelle als eth0 konfigurieren.



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 Secure Network Analytics das Verhalten identifiziert hat, kann das System alle Maßnahmen ergreifen, die Sie gegebenenfalls für diese Art von Verhalten konfiguriert haben.

UDP Director 2210

Der 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 verwenden, müssen Sie zwei UDP Director-Appliances über Crossover-Kabel verbinden. Anweisungen finden Sie unter [2. Verbinden Ihrer Appliance mit dem Netzwerk](#).

Flow Sensor 1210, 3210 und 4240

Der 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:

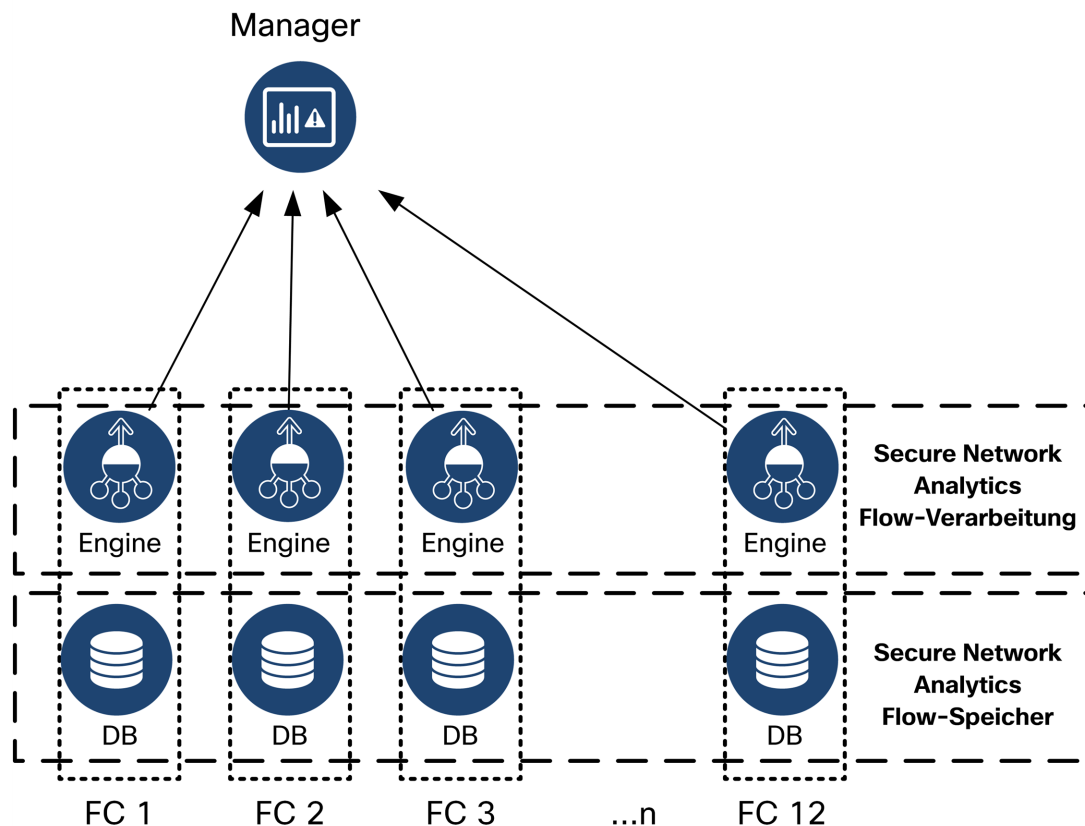
- Bereiche, in denen NetFlow nicht verfügbar ist
- Bereiche, in denen NetFlow verfügbar ist, Sie aber einen besseren Überblick über Performancemetriken und Paketdaten wünschen.

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 Secure Network Analytics Flow Collector bietet der Flow Sensor auch einen detaillierten Einblick in Performancemetriken und Verhaltensindikatoren. Diese Flow-Leistungskennzahlen geben Aufschluss über jede Roundtrip-Latenz, die durch das Netzwerk oder die serverseitige Anwendung verursacht wird.

Da der Flow Sensor auf Paketebene sichtbar ist, kann er die Roundtrip-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.

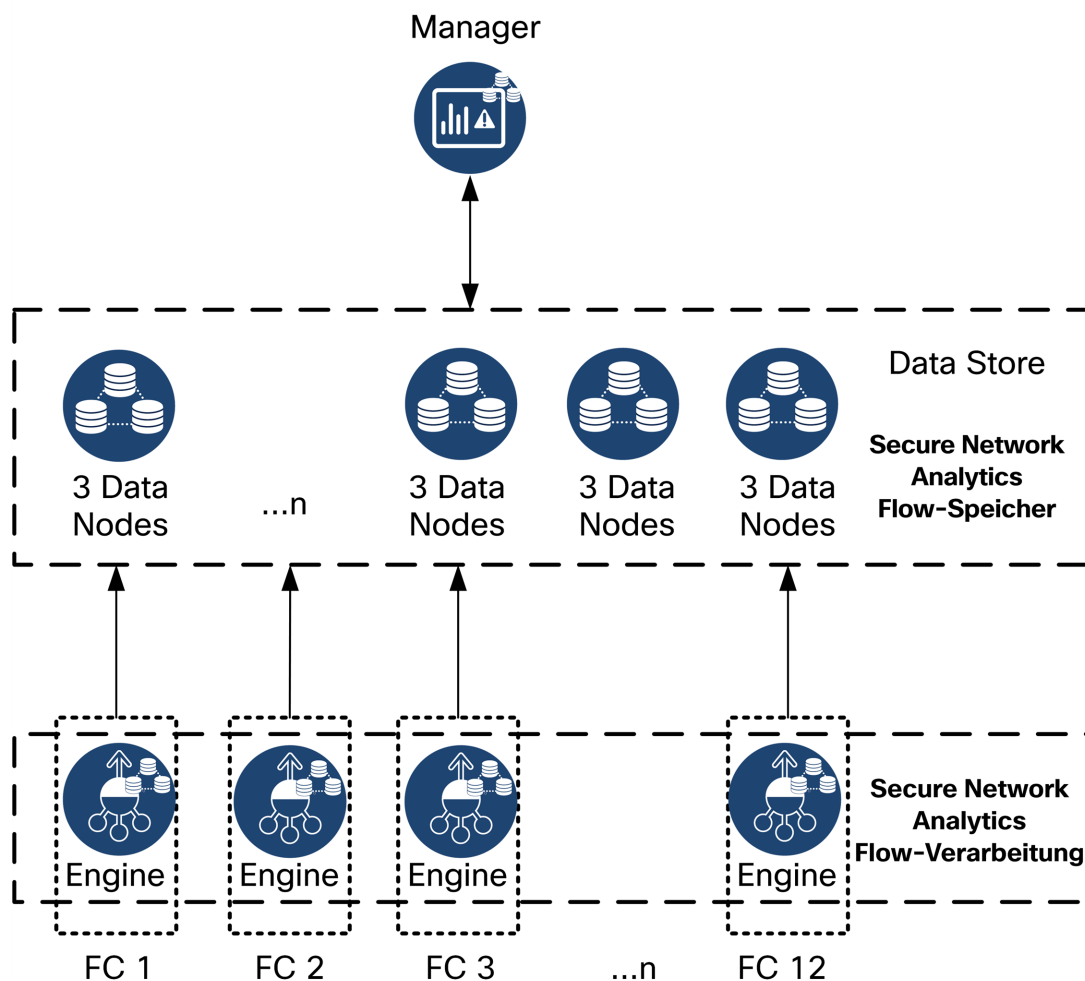
Secure Network Analytics ohne Data Store

In einer Secure Network Analytics-Bereitstellung ohne Data Store erfassen ein oder mehrere Flow Collectors Daten und deduplizieren sie, führen Analysen durch und melden Daten und Ergebnisse direkt an den Manager. Um von Benutzern ausgehende Abfragen, einschließlich Grafiken und Diagrammen, aufzulösen, fragt der Manager alle verwalteten Flow Collectors ab. Jeder Flow Collector gibt passende Ergebnisse an den Manager zurück. Der Manager stellt die Informationen aus den verschiedenen Ergebnissätzen zusammen und erzeugt dann eine Grafik oder ein Diagramm mit den Ergebnissen. Bei dieser Bereitstellung speichert jeder Flow Collector Daten in einer lokalen Datenbank. Nehmen Sie das folgende Diagramm als Beispiel.



Secure Network Analytics mit Data Store

In einer Secure Network Analytics-Bereitstellung mit einem Data Store befindet sich der Data Store-Cluster zwischen dem Manager und den Flow Collectors. Ein oder mehrere Flow Collectors erfassen Flows und deduplizieren sie, führen Analysen durch und melden Daten und Ergebnisse direkt an den Data Store, wobei sie ungefähr gleichmäßig auf alle Data Nodes verteilt werden. Der Data Store erleichtert die Datenspeicherung, hält Ihren gesamten Datenverkehr an diesem zentralen Ort, anstatt ihn über mehrere Flow Collectors zu verteilen, und bietet eine größere Speicherkapazität als mehrere Flow Collectors. Nehmen Sie das folgende Diagramm als Beispiel.



Der Data Store bietet ein zentrales Repository zum Speichern der Telemetriedaten Ihres Netzwerks, die vom Flow Collector erfasst werden. Der Data Store besteht aus einem Cluster von Data Nodes, die jeweils einen Teil Ihrer Daten enthalten, und einem Backup von Daten eines separaten Data Node. Da sich alle Ihre Daten in einer zentralen Datenbank befinden und nicht über mehrere Flow Collectors verteilt sind, kann der

Manager Abfrageergebnisse vom Data Store schneller abrufen, als wenn alle Flow Collectors separat abgefragt würden. Der Data Store-Cluster bietet eine verbesserte Fehlertoleranz, eine verbesserte Antwort auf Abfragen und eine schnellere grafische Darstellung.

Abfragen

Um von Benutzern ausgehende Abfragen, einschließlich Grafiken und Diagrammen, aufzulösen, fragt der Manager den Data Store ab. Der Data Store sucht in den für die Abfrage relevanten Spalten nach passenden Ergebnissen, ruft dann die entsprechenden Zeilen ab und gibt die Abfrageergebnisse an den Manager zurück. Der Manager generiert die Grafik oder das Diagramm, ohne dass mehrere Ergebnissätze von mehreren Flow Collectors zusammengestellt werden müssen. Dies reduziert die Abfragekosten im Vergleich zur Abfrage mehrerer Flow Collectors und verbessert die Abfrageleistung.

Data Store-Speicherung und Fehlertoleranz

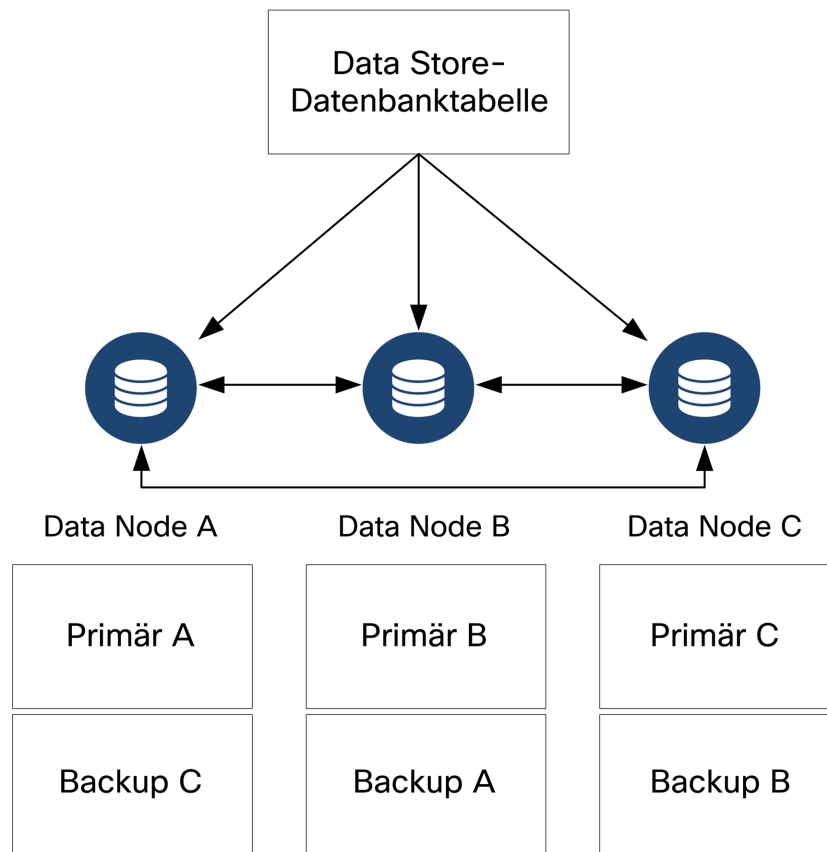
Der Data Store sammelt Daten von Flow Collectors und verteilt sie gleichmäßig auf Data Nodes innerhalb des Clusters. Jeder Data Node speichert nicht nur einen Teil Ihrer Gesamttelemetrie, sondern auch eine Sicherungskopie der Telemetrie eines anderen Data Nodes. Speichern von Daten auf diese Weise:

- erleichtert die Lastverteilung
- verteilt die Verarbeitung auf jeden Knoten
- stellt sicher, dass alle Daten, die der Data Store erfasst, ein Backup für Fehlertoleranz haben
- ermöglicht die Erhöhung der Anzahl von Data Nodes zur Verbesserung der gesamten Speicher- und Abfrageleistung

Wenn Ihr Data Store über drei oder mehr Data Nodes verfügt und ein Data Node ausfällt, bleibt der gesamte Data Store aktiv, solange der Knoten, der seine Sicherung enthält, noch verfügbar ist und mindestens die Hälfte Ihrer gesamten Data Nodes noch in Betrieb ist. So haben Sie Zeit, die ausgefallene Verbindung oder fehlerhafte Hardware zu reparieren. Nachdem Sie den fehlerhaften Data Node ersetzt haben, stellt der Data Store die Daten dieses Knotens aus der vorhandenen Sicherung wieder her, die auf dem benachbarten Data Node gespeichert ist, und erstellt eine Sicherung der Daten auf diesem Data Node.

Beispiel für Telemetriespeicher

Im folgenden Diagramm finden Sie ein Beispiel dafür, wie 3 Data Nodes Telemetrie speichern:



Allgemeine Bereitstellungsanforderungen

Bevor Sie beginnen, lesen Sie diesen Leitfaden, um den Prozess sowie die Vorbereitung, den Zeitaufwand und die Ressourcen zu verstehen, die Sie für die Planung der Installation benötigen.

Installationsmethoden

Sie können eine VMware-Umgebung oder KVM (Kernel-based Virtual Machine) für die Installation der virtuellen Appliance verwenden.



Lesen Sie vor der Installation die in den folgenden Abschnitten angegebenen Informationen zu **Kompatibilität** und **Ressourcenanforderungen**.

Methoden	Installationsanweisungen (als Referenz)	Installationsdatei	Details
VMware vCenter	3a) Installieren einer virtuellen Appliance mit VMware vCenter (ISO)	ISO	Installieren Ihrer virtuellen Appliances mit VMware vCenter.
Eigenständiger VMware ESXi-Server	3b) Installieren einer virtuellen Appliance auf einem eigenständigen ESXi-Server (ISO)	ISO	Installieren Ihrer virtuellen Appliances auf einem eigenständigen ESXi-Hostserver.
KVM und Virtual Machine Manager	3c) Installieren einer virtuellen Appliance auf einem KVM-Host (ISO)	ISO	Installieren Ihrer virtuellen Appliances mit KVM und Virtual Machine Manager.

Kompatibilität

Unabhängig davon, ob Sie Ihre virtuellen Appliances in einer VMware-Umgebung oder einer KVM (Kernel-based Virtual Machine) installieren möchten, sollten Sie die folgenden Kompatibilitätsinformationen beachten:

Allgemeine Anforderungen für alle Appliances

Anforderung	Beschreibung
Dedizierte Ressourcen	Alle Appliances erfordern die Zuweisung dedizierter Ressourcen und können nicht mit anderen Appliances oder Hosts gemeinsam genutzt werden.
Keine Live-Migration	Appliances unterstützen vMotion aufgrund der Möglichkeit von Beschädigung nicht.
Netzwerkadapter	Alle Appliances benötigen mindestens 1 Netzwerkadapter. Flow Sensors können mit zusätzlichen Adapters konfiguriert werden, um zusätzlichen Durchsatz zu unterstützen. Data Nodes benötigen einen zweiten Netzwerkadapter für die Kommunikation mit anderen Data Nodes als Teil des Data Store.
Storage-Controller	Wählen Sie bei der Konfiguration der ISO-Datei in VMware <code>LSI Logic SAS</code> als SCSI-Controller -Typ aus.
Speicherbereitstellung	Weisen Sie bei der Bereitstellung virtueller Appliances „Thick Provisioned Lazy Zeroed“-Speicherbereitstellung zu.
CPU-Befehlssatz-Anforderung	Stellen Sie sicher, dass Ihre CPU die AVX/AVX2-Befehlssätze ausführen kann. Wählen Sie für ESXi die VM-Hardwareversion 11 oder höher aus. Für KVM empfehlen wir Host-Passthrough.

VMware

- **Kompatibilität:** VMware 7.0 oder 8.0
- **Betriebssystem:** Debian 11 (64 Bit)
- **Netzwerkadapter:** Für optimale Leistung wird der Adaptertyp VMXNET3 empfohlen.
- **ISO-Bereitstellung:** Secure Network Analytics 7.5.0 ist mit VMware 7.0 und 8.0 kompatibel. VMware 6.0, 6.5 und 6.7 werden von Secure Network Analytics 7.5.x nicht unterstützt. Weitere Informationen finden Sie in der VMware-Dokumentation zum Ende des allgemeinen Supports für vSphere 6.0, 6.5 und 6.7.
- **Live-Migration:** Live-Migration (z. B. mit vMotion) von Host zu Host wird nicht unterstützt.
- **Snapshots:** Snapshots von Virtual Machines werden nicht unterstützt.



Installieren Sie VMware Tools nicht auf einer virtuellen Secure Network Analytics-Appliance, da dadurch die bereits installierte angepasste Version überschrieben wird. Dies würde die virtuelle Appliance funktionsunfähig machen und eine Neuinstallation erfordern.

KVM

- **Kompatibilität:** Sie können jede kompatible Linux-Distribution verwenden.
- **KVM-Host-Versionen:** Es gibt mehrere Methoden, um eine Virtual Machine auf einem KVM-Host zu installieren. Wir haben KVM getestet und die Leistung mit den folgenden Komponenten validiert:
 - libvirt 2.10 bis 7.1.0
 - qemu-KVM 2.6.1 bis 5.2.0
 - Open vSwitch 2.6.x bis 2.15.x****
 - Linux Kernel 4.4.x und tw. 5.10.x
- **Betriebssystem:** Debian 11 (64 Bit)
- **Virtualisierungs-Host:** Mindestanforderungen und Anforderungen für optimale Leistung finden Sie im Abschnitt **Ressourcenanforderungen** und im Hardware-Spezifikationsblatt für Ihre Appliance unter [Cisco.com](https://www.cisco.com).



Die Systemleistung wird durch die Hostumgebung bestimmt. Ihre Leistung kann variieren.

Software herunterladen

Verwenden Sie Cisco Software Central, um Installationsdateien, Patches und Software-Update-Dateien für virtuelle Appliances (VE) herunterzuladen. Melden Sie sich unter <https://software.cisco.com> bei Ihrem Cisco Smart Account an oder wenden Sie sich an Ihren Administrator. Siehe **2. Herunterladen der Installationsdateien für die Virtual Edition** für Anweisungen.

TLS

Sie können die TLS-Versionskonfiguration für Ihre Appliances wie folgt auswählen:

- TLS 1.2 und 1.3 (Standard)
- Nur TLS 1.3 (nicht unterstützt für Data Store)

Anwendungen von Drittanbietern

Secure Network Analytics unterstützt keine Installation von Drittanbieter-Anwendungen auf Appliances.

Browser

- **Kompatibler Browser:** Secure Network Analytics unterstützt die neuesten Versionen von Chrome, Firefox und Edge.
- **Microsoft Edge:** Bei Microsoft Edge kann es zu einer Beschränkung der Dateigröße kommen. Wir raten davon ab, Microsoft Edge zum Installieren der ISO-Dateien für die Virtual Edition zu verwenden.

Hostname

Für jede Appliance ist ein eindeutiger Hostname erforderlich. Wir können keine Appliance mit demselben Hostnamen wie eine andere Appliance konfigurieren. Stellen Sie außerdem sicher, dass jeder Hostname der Appliance die Internetstandardanforderungen für Internethosts erfüllt.

Domänenname

Für jede Appliance ist ein vollständig qualifizierter Domänenname erforderlich. Wir können keine Appliance mit einer leeren Domäne installieren.

NTP-Server

- **Konfiguration:** Für jede Appliance ist mindestens 1 NTP-Server erforderlich.
- **Problematischer NTP:** Entfernen Sie den NTP-Server 130.126.24.53, wenn er in Ihrer Serverliste aufgeführt ist. Dieser Server ist bekanntermaßen problematisch und wird in unserer Standardliste von NTP-Servern nicht mehr unterstützt.

Zeitzone

Bei allen Secure Network Analytics-Appliances wird die koordinierte Weltzeit (UTC) verwendet.

- **Virtueller Hostserver:** Stellen Sie sicher, dass auf Ihrem virtuellen Hostserver die richtige Uhrzeit eingestellt ist.



Stellen Sie sicher, dass die Zeiteinstellung auf dem virtuellen Hostserver (auf dem Sie die virtuellen Appliances installieren werden) richtig ist. Andernfalls können die virtuellen Appliances möglicherweise nicht gestartet werden.

Standard-Appliance-Anforderungen (ohne Data Store)

Wenn Sie Secure Network Analytics ohne Data Store installieren, installieren Sie die folgenden Appliances:

Appliance	Anforderung
Manager	• Mindestens 1 Manager
Flow Collector	• Mindestens 1 Flow Collector
UDP Director	Optional
Flow Sensor	Optional

Informationen zu den Appliance-Anforderungen für die Installation von Secure Network Analytics mit einem Data Store finden Sie unter [Data Store-Bereitstellungsanforderungen](#).

Manager- und Flow Collector-Bereitstellungsanforderungen

Für jeden Manager und jeden Flow Collector, den Sie bereitstellen, müssen Sie dem Management-Port `eth0` eine öffentliche, routbare IP-Adresse zuweisen.

Data Store-Bereitstellungsanforderungen

Überprüfen Sie zur Bereitstellung von Secure Network Analytics mit einem Data Store die folgenden Voraussetzungen und Empfehlungen.

Appliance-Anforderungen (mit Data Store)

Die folgende Tabelle gibt einen Überblick über die erforderlichen Appliances für die Bereitstellung von Secure Network Analytics mit einem Data Store.

Appliance	Anforderung
Manager	<ul style="list-style-type: none"> • Mindestens 1 Manager
Data Store	<ul style="list-style-type: none"> • Mindestens 1 oder 3 Data Nodes • Zusätzliche Sätze von jeweils drei 3 Data Nodes zur Erweiterung des Data Store, maximal 36 Data Nodes • Die Bereitstellung von nur 2 Data Nodes in einem Cluster wird nicht unterstützt.
Flow Collector	<ul style="list-style-type: none"> • Mindestens 1 Flow Collector
Flow Sensor	Optional



Aktualisieren Sie das Appliance-BIOS nicht, da dies zu Problemen mit der Appliance-Funktionalität führen kann.

Manager- und Flow Collector-Bereitstellungsanforderungen


Für jeden Manager und jeden Flow Collector, den Sie bereitstellen, müssen Sie dem Management-Port `eth0` eine öffentliche, routbare IP-Adresse zuweisen.

- **Konfiguration des eth0-Ports:** Sie können die Verwendung eines **BASE-T-Kupfer-1G/10G-Ports** oder eines **SFP+-Twinax-Kabel-10G-Ports** für den `eth0`-Managementport des Managers und des Flow Collectors konfigurieren.
- **Durchsatz:** Für den BASE-T-Kupfer-Port ist bei Verwendung eines Data Store ein 10G-Durchsatz erforderlich. Wenn Sie keinen Data Store bereitstellen, können Sie nur die 100-Mbit/s-/1-Gbit/s-/10-Gbit/s-Kupferschnittstelle als `eth0` konfigurieren.

Data Node-Bereitstellungsanforderungen

Jeder Data Store besteht aus Data Nodes.

- **Hardware:** Jeder Hardware-Data Node ist sein eigenes Chassis. Sie können 1, 3 oder mehr Data Nodes (in Dreiergruppen) bereitstellen.
- **Virtual Edition:** Wenn Sie einen virtuellen Data Store herunterladen, können Sie 1, 3 oder mehr Data Nodes der Virtual Edition (in Dreiergruppen) bereitstellen.

 Stellen Sie sicher, dass es sich bei Ihren Data Nodes ausschließlich um Hardware-Data Nodes oder ausschließlich um Data Nodes der Virtual Edition handelt. Die gemeinsame Verwendung von Hardware-Data Nodes und virtuellen Data Nodes wird nicht unterstützt und die Hardware muss aus derselben Hardware-Generation stammen (alle DS 6200 oder alle DN 6300).

Bereitstellung mehrerer Data Nodes

Eine Bereitstellung mit mehreren Data Nodes bietet maximale Leistung. Eine Data Store-Bereitstellung mit 3 Data Nodes kann beispielsweise etwa 1,5 Millionen Flows pro Sekunde verarbeiten und diese Daten etwa 90 Tage aufbewahren.

Beachten Sie Folgendes:

- **Dreiergruppen:** Die Data Nodes können als Teil Ihres Data Store in Dreiergruppen geclustert werden, von einem Minimum von 3 bis zu einem Maximum von 36. Die Bereitstellung von nur 2 Data Nodes in einem Cluster wird nicht unterstützt.
- **Ausschließlich Hardware-Data Nodes oder ausschließlich virtuelle Data Nodes:** Stellen Sie sicher, dass es sich bei Ihren Data Nodes ausschließlich um Hardware-Data Nodes (derselben Generation) oder ausschließlich um Data Nodes der Virtual Edition handelt. Das Mischen von Hardware und virtuellen Data Nodes oder das Mischen von Data Store 6200 und Data Node 6300 Data Nodes wird nicht unterstützt.

Unterstützte Hardwaremetriken (mit aktivierter Analytik)

Anzahl der Knoten	Flows pro Sekunde	Eindeutige interne Hosts
1	600.000	1,3 Millionen
3 und höher	600.000	1,3 Millionen
3 und höher	850.000	700.000

i Diese Empfehlungen berücksichtigen nur die Telemetrie. Ihre Leistung kann in Abhängigkeit von weiteren Faktoren variieren, einschließlich der Anzahl der Hosts, der Verwendung von Flow Sensors, Datenverkehrsprofilen und anderen Netzwerkmerkmalen. Wenden Sie sich an [Cisco Support](#), wenn Sie Hilfe bei der Dimensionierung benötigen.

Unterstützte Hardwaremetriken (ohne aktivierte Analytik)

Anzahl der Knoten	Flows pro Sekunde	Eindeutige interne Hosts
1	Bis zu 1 Million	Bis zu 33 Millionen
3 und höher	Bis zu 3 Millionen	Bis zu 33 Millionen

i Diese Zahlen werden in unseren Testumgebungen anhand durchschnittlicher Kundendaten mit 1,3 Millionen eindeutigen Hosts erzeugt. Es gibt mehrere Faktoren, die sich auf Ihre spezifische Leistung auswirken können, z. B. die Anzahl der Hosts, die durchschnittliche Flow-Größe und mehr. Wenden Sie sich an [Cisco Support](#), wenn Sie Hilfe bei der Dimensionierung benötigen.

Bereitstellung einzelner Data Nodes

Wenn Sie einen einzelnen (1) Data Node bereitstellen möchten, müssen Sie Folgendes beachten:

- **Flow Collectors:** Es werden maximal 4 Flow Collectors unterstützt.
- **Hinzufügen von Data Nodes:** Wenn Sie nur einen Data Node bereitstellen, können Sie Ihrer Bereitstellung später weitere Data Nodes hinzufügen. Weitere Informationen finden Sie unter [Bereitstellung mehrerer Data Nodes](#).

Diese Empfehlungen berücksichtigen nur die Telemetrie. Ihre Leistung kann in Abhängigkeit von weiteren Faktoren variieren, einschließlich der Anzahl der Hosts, der Verwendung von Flow Sensors, Datenverkehrsprofilen und anderen Netzwerkmerkmalen. Wenden Sie sich an den [Cisco Support](#), wenn Sie Hilfe bei der Dimensionierung benötigen.

Zurzeit unterstützt der Data Store keine Bereitstellung von Data Node als automatischen Ersatz, wenn ein primärer Data Node ausfällt. Wenden Sie sich an den [Cisco Support](#), wenn Sie Hilfe benötigen.

Data Node-Konfigurationsanforderungen

Um einen Data Store bereitzustellen, müssen Sie jedem Data Node die nachfolgenden Elemente zuweisen. Die von Ihnen vorbereiteten Informationen werden bei der Ersteinrichtung mithilfe des [Systemkonfigurationshandbuchs](#) konfiguriert.

- **Routbare IP-Adresse (eth0):** Für die Management-, Erfassungs- und Abfragekommunikation mit Ihren Secure Network Analytics-Appliances.
- **Konfiguration des eth0-Ports:** Sie können bei allen unterstützten Transceivern die Verwendung eines **BASE-T**-Kupfer-1G/10G-Ports oder eines SFP+-Twinax-Kabel-10G-Ports für den eth0-Managementport konfigurieren.
- **Durchsatz:** Für den BASE-T-Kupfer-Port ist bei Verwendung eines Data Store ein 10G-Durchsatz erforderlich.
- **Kommunikation zwischen Data Nodes:** Konfigurieren Sie eine nicht routbare IP-Adresse aus dem CIDR-Block 169.254.42.0/24 in einem privaten LAN oder VLAN für die Kommunikation zwischen Data Nodes.

Verbinden Sie den Data Node-eth2-Port (oder den Port-Channel, der eth2 und eth3 enthält) mit den Switches für die Kommunikation zwischen Data Nodes, um die Durchsatzleistung zu verbessern. Als Teil des Data Store kommunizieren Ihre Data Nodes untereinander.

- **Netzwerkverbindungen:** Sie benötigen zwei 10G-Netzwerkverbindungen – eine für die Management-, Erfassungs- und Abfragekommunikation und eine für die Kommunikation zwischen Data Nodes.
- **Zusätzliche Verbindung und Switch:** Installieren Sie optional (nur bei Hardware-Data Nodes) für Netzwerkredundanz und Kritikalität der Kommunikation zwischen Data Nodes eine zusätzliche 10G-Verbindung und einen zusätzlichen Switch zum Aufbau eines Port-Channels auf dem Data Node.



Konfigurieren Sie Ihre Data Nodes so, dass die benachbarten Data Nodes mit separaten, redundanten Netzteilen versorgt werden. Diese Konfiguration verbessert die Datenredundanz und die Gesamtbetriebszeit des Data Store.

Überlegungen zu Netzwerk und Switching

Die folgende Tabelle gibt einen Überblick über die Netzwerk- und Switching-Überlegungen bei der Bereitstellung von Secure Network Analytics mit einem Data Store.

Überlegungen zum Netzwerk	Beschreibung
Kommunikation zwischen Data Nodes	<ul style="list-style-type: none"> • Legen Sie eine empfohlene Roundtrip-Zeit-Latenz (RTT) unter 200 Mikrosekunden zwischen den Data Nodes fest. • Begrenzen Sie den Zeitversatz zwischen Ihren Data Nodes auf 1 Sekunde oder weniger. • Stellen Sie einen empfohlenen Durchsatz von 6,4 Gbit/s oder mehr (10 Gbit/s Vollduplex-Switch-Verbindung) zwischen Ihren Data Nodes her. • Für Hardware-Data Nodes ist die Konfiguration eines <code>eth2</code>-Ports für 10G-Durchsatz für die normale Kommunikation zwischen Data Nodes ausreichend. Die Erstellung eines <code>LACP-eth2/eth3</code>-Port-Channels für bis zu 20G-Durchsatz ermöglicht eine schnellere Kommunikation der Data Nodes untereinander und ein schnelleres Hinzufügen oder Ersetzen von Data Nodes zum Data Store, da jeder neue Data Node Datenverkehr von benachbarten Data Nodes erhält, um seine Daten aufzufüllen. Beachten Sie, dass LACP-Port-Bonding die einzige verfügbare Bonding-Option für Hardware-Data Nodes ist.

Stromversorgung der Data Node-Hardware	<ul style="list-style-type: none"> • Wenn unerwartet der Strom bei einem Hardware-Data Node ausfällt, können die Daten beschädigt werden. Verwenden Sie beide Netzteile an von unterbrechungsfreien Stromversorgungen getrennten Stromkreisen. • Wenn Sie den Data Store-Cluster initialisieren, wechseln Sie die Data Node-Konfiguration basierend auf den Netzteilen, die jeder Data Node verwendet, ab. Dies kann die Fehlertoleranz optimieren, indem die Anzahl der Data Nodes, die bei einem Stromausfall ausfallen, minimiert wird.
Data Node-Switching	<ul style="list-style-type: none"> • Data Nodes benötigen ihr eigenes Layer-2-VLAN, um die Kommunikation zwischen Data Nodes zu ermöglichen. Hardware-Data Nodes können an einen gemeinsamen oder dedizierten 10G-Switch angeschlossen werden. • Wir empfehlen, die Hardware-Data Nodes an 2 Switches anzuschließen, um eine konstante Netzwerkverbindung bei Switch-Ausfällen und -Upgrades zu gewährleisten. Aufgrund der geringen Latenz, die für die Kommunikation zwischen Data Nodes erforderlich ist, empfiehlt Cisco ein redundantes Switch-Paar, bei dem die beiden Switches miteinander verbunden sind und das Layer-2-VLAN über beide Switches übertragen.
Secure Network Analytics Appliance-Kommunikation	<ul style="list-style-type: none"> • Der Manager und die Flow Collectors müssen in der Lage sein, alle Data Nodes zu erreichen. • Die Data Nodes müssen in der Lage sein, den Manager, alle Flow Collectors und jeden Data Node zu erreichen.



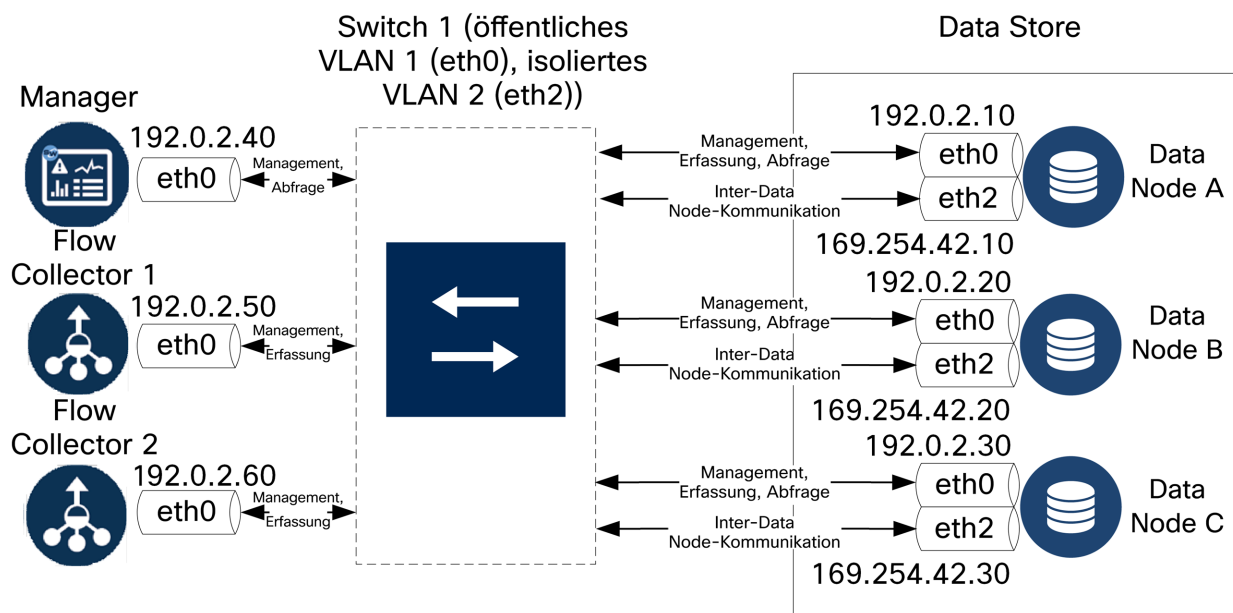
Zurzeit unterstützt der Data Store keine Bereitstellung von Data Node als automatischen Ersatz, wenn ein primärer Data Node ausfällt. Wenden Sie sich an den [Cisco Support](#), wenn Sie Hilfe benötigen.

Hardware-Switch – Beispiel

Um die Kommunikation zwischen Data Nodes über `eth2` oder den Port-Channel `eth2/eth3` zu ermöglichen, müssen Sie einen Switch bereitstellen, der 10G-Geschwindigkeiten unterstützt.

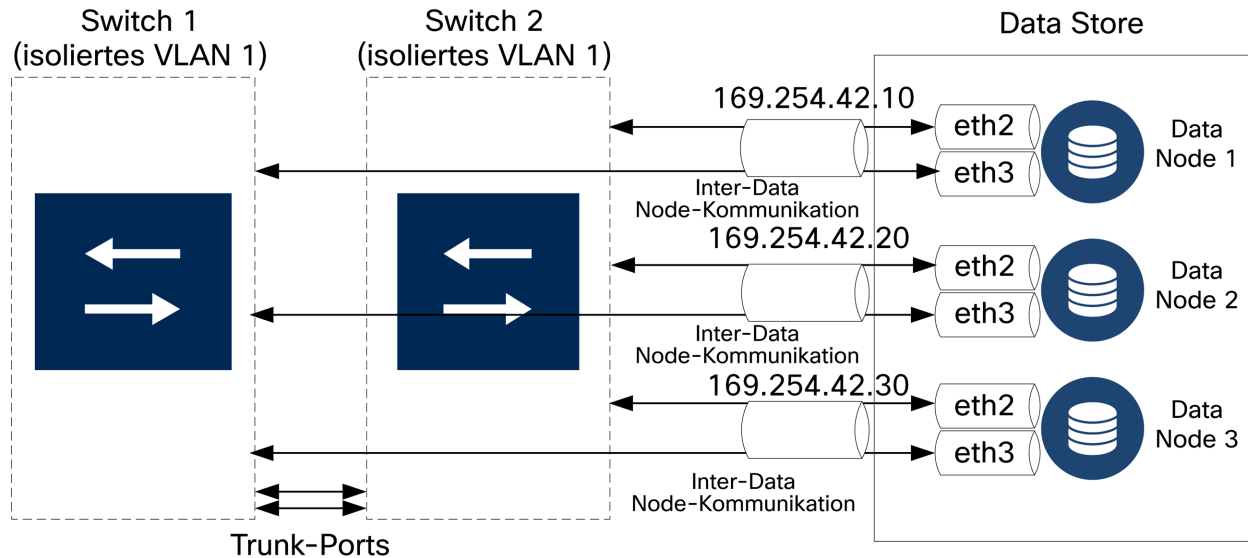
Konfigurieren Sie ein LAN oder VLAN für die `eth0`-Kommunikation der Data Nodes mit dem Manager und den Flow Collectors und ein isoliertes LAN oder VLAN für die Kommunikation zwischen Data Nodes.

Sie können diese Switches mit anderen Appliances gemeinsam nutzen, aber separate LANs oder VLANs für den zusätzlichen Appliance-Datenverkehr erstellen. Nehmen Sie das folgende Diagramm als Beispiel.



Das Data Store-Cluster benötigt einen kontinuierlichen Heartbeat zwischen den Knoten innerhalb des isolierten VLANs. Ohne diesen Heartbeat können Data Nodes offline gehen, was das Risiko eines Data Store-Ausfalls erhöht.

Wenn Sie zusätzliche Netzwerkredundanz wünschen, um Switch-Updates und geplante Ausfälle zu berücksichtigen, müssen Sie Ihre Data Nodes mit Port-Channels für die dedizierte Kommunikation zwischen Data Nodes konfigurieren. Verbinden Sie jeden Data Node mit 2 Switches, wobei jeder physikalische Port mit einem anderen Switch verbunden ist. Nehmen Sie das folgende Diagramm als Beispiel.



Wenden Sie sich an Cisco Professional Services, um Unterstützung bei der Planung Ihrer Bereitstellung zu erhalten.

Überlegungen zur Data Store-Platzierung

Platzieren Sie jeden Data Node so, dass er mit allen Ihren Flow Collectors, dem Manager und jedem anderen Data Node kommunizieren kann. Die beste Leistung erzielen Sie durch eine Co-Location Ihrer Data Nodes und Flow Collectors, um die Kommunikationslatenz zu minimieren, sowie einer Co-Location Ihrer Data Nodes und des Managers für eine optimale Abfrageleistung.

- **Firewall:** Es wird dringend empfohlen, die Data Nodes innerhalb Ihrer Firewall zu platzieren, z. B. innerhalb eines NOC.
- **Stromversorgung:** Wenn der Data Store aufgrund eines Stromausfalls oder Hardwarefehlers ausfällt, besteht ein erhöhtes Risiko von Datenbeschädigungen und Datenverlust. Installieren Sie Ihre Data Nodes so, dass eine konstante Betriebszeit gewährleistet ist.

Wenn unerwartet die Stromversorgung eines Data Node ausfällt und Sie die Appliance neu starten, wird die Datenbankinstanz auf diesem Data Node möglicherweise nicht automatisch neu gestartet. Informationen zur Fehlerbehebung und zum manuellen Neustart der Datenbank finden Sie im [Systemkonfigurationshandbuch](#).

- **Richtlinie:** Prüfen Sie, ob die Richtlinie für die Wiederherstellung der Data Node-Stromversorgung auf **Restore Last State** (Letzten Status wiederherstellen) eingestellt ist. Dadurch wird der Data Node nach einem Stromausfall automatisch neu gestartet und versucht, laufende Prozesse wiederherzustellen. Weitere Informationen zum Konfigurieren der Richtlinie für die Wiederherstellung der Stromversorgung in CIMC finden Sie im [Konfigurationsleitfaden für die GUI der Cisco UCS C-Series](#).

Die Analytik der Bereitstellungsanforderungen

Secure Network Analytics verwendet dynamische Entitätsmodellierung, um den Status Ihres Netzwerks zu verfolgen. Im Zusammenhang mit Secure Network Analytics ist eine Entität etwas, das im Laufe der Zeit verfolgt werden kann, z. B. ein Host oder Endpunkt in Ihrem Netzwerk. Die dynamische Entitätsmodellierung erfasst Informationen über Entitäten basierend auf dem übertragenen Datenverkehr und den Aktivitäten, die sie in Ihrem Netzwerk durchführen. Weitere Informationen finden Sie im [Leitfaden zur Analytik: Erkennung, Warnungen und Beobachtungen](#).

Um die Analytik zu aktivieren, muss Ihre Bereitstellung

- in einer virtuellen oder Hardware-Data Store-Bereitstellung mit einer beliebigen Anzahl von Flow Collectors konfiguriert sein.
- mit nur 1 Data Store-Domäne Secure Network Analytics.

1. 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 die Informationen in diesem Abschnitt, um Ihr Netzwerk so zu konfigurieren, dass die Appliances über das Netzwerk kommunizieren können.

Offene Ports (alle Appliances)

Wenden Sie sich an Ihren Netzwerkadministrator, um sicherzustellen, dass die folgenden Ports offen sind und uneingeschränkten Zugriff auf Ihre Appliances (Manager, Flow Collectors, Data Nodes, Flow Sensors und UDP Directors) haben:

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

Zusätzliche offene Ports für Data Nodes

Wenn Sie Data Nodes in Ihrem Netzwerk bereitstellen, stellen Sie außerdem sicher, dass die folgenden Ports offen sind und uneingeschränkten Zugriff haben:

- TCP 5433
- TCP 5444
- TCP 9450

Kommunikations -Ports und Protokolle

Die folgende Tabelle zeigt, wie die Ports in Secure Network Analytics 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	Manager	TCP/389, UDP/389	LDAP
Cisco ISE	Manager	TCP/443	HTTPS
Cisco ISE	Manager	TCP/8910	XMPP
Externe Protokollquellen	Manager	UDP/514	SYSLOG
Flow Collector	Manager	TCP/443	HTTPS
UDP Director	Manager	TCP/443	HTTPS
UDP Director	Flow Collector (sFlow)	UDP/6343*	sFlow
UDP Director	Flow Collector (NetFlow)	UDP/2055*	NetFlow
UDP Director	Ereignismanagement-Systeme von Drittanbietern	UDP/514	SYSLOG
Flow Sensor	Manager	TCP/443	HTTPS
Flow Sensor	Flow Collector (NetFlow)	UDP/2055	NetFlow
NetFlow-Exporter	Flow Collector (NetFlow)	UDP/2055*	NetFlow
sFlow-Exporter	Flow Collector (sFlow)	UDP/6343*	sFlow
Manager	UDP Director	TCP/443	HTTPS

Von (Client)	An (Server)	Port	Protokoll
Manager	Cisco ISE	TCP/443	HTTPS
Manager	Cisco ISE	TCP/8910	XMPP
Manager	DNS	UDP/53	DNS
Manager	Flow Collector	TCP/443	HTTPS
Manager	Flow Sensor	TCP/443	HTTPS
Manager	Flow-Exporter	UDP/161	SNMP
Manager	LDAP	TCP/636	TLS
Manager	CRL-Verteilungspunkte	TCP/80	HTTP
Manager	OCSP-Responder	TCP/80	OCSP
Benutzer-PC	Manager	TCP/443	HTTPS

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

Zusätzliche offene Ports für Data Store

Im Folgenden sind die Kommunikations-Ports aufgelistet, die auf Ihrer Firewall geöffnet werden müssen, um den Data Store bereitzustellen.

#	Von (Client)	An (Server)	Port	Protokoll oder Zweck
1	Manager	Flow Collectors und Data Nodes	22/TCP	SSH, erforderlich zum Initialisieren der Data Store-Datenbank
1	Data Nodes	alle anderen Data Nodes	22/TCP	SSH, erforderlich zum Initialisieren der Data Store-Datenbank und für Datenbankadministrationsaufgaben
2	Manager, Flow Collectors und Data Nodes	NTP-Server	123/UDP	NTP, erforderlich für die Zeitsynchronisierung
2	NTP server	Manager, Flow Collectors und Data Nodes	123/UDP	NTP, erforderlich für die Zeitsynchronisierung
3	Manager	Flow Collectors und Data Nodes	443/TCP	HTTPS, erforderlich für die sichere Kommunikation zwischen Appliances
3	Flow Collectors	Manager	443/TCP	HTTPS, erforderlich für die sichere Kommunikation zwischen Appliances
3	Data Nodes	Manager	443/TCP	HTTPS, erforderlich für die sichere Kommunikation zwischen Appliances

4	NetFlow-Exporter	Flow Collectors - NetFlow	2055/UDP	NetFlow-Erfassung
5	Data Nodes	alle anderen Data Nodes	4803/TCP	Inter-Data Node-Messaging-Dienst
6	Data Node	alle anderen Data Nodes	4803/UDP	Inter-Data Node-Messaging-Dienst
7	Data Nodes	alle anderen Data Nodes	4804/UDP	Inter-Data Node-Messaging-Dienst
8	Manager, Flow Collectors und Data Nodes	Data Nodes	5433/TCP	Vertica Client-Verbindungen
9	Data Node	alle anderen Data Nodes	5433/UDP	Vertica Messaging-Dienst-Monitoring
10	sFlow-Exporter	Flow Collector (sFlow)	6343/UDP	sFlow-Erfassung
11	Data Nodes	alle anderen Data Nodes	6543/UDP	Inter-Data Node-Messaging-Dienst

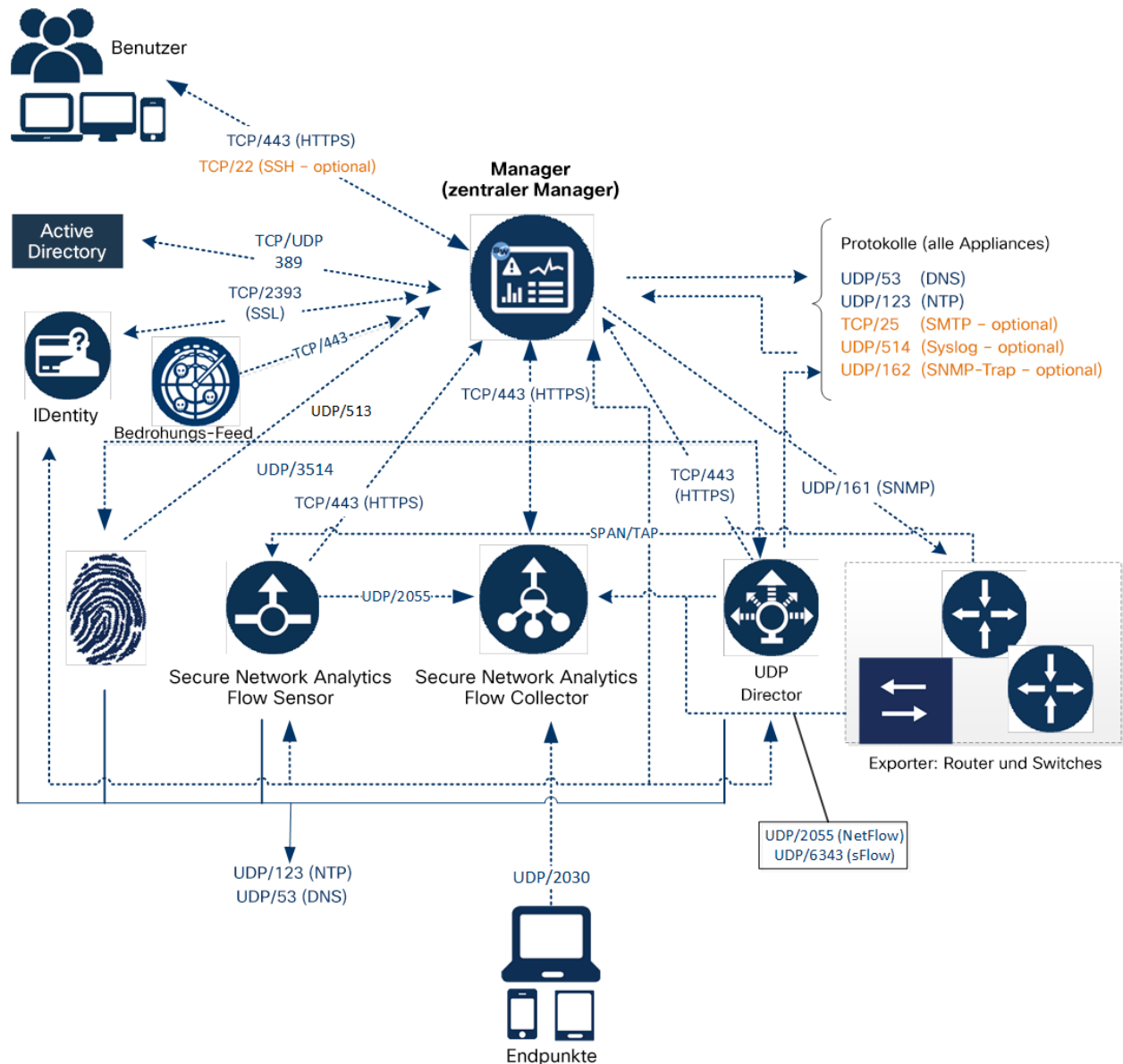
Optionale Kommunikations-Ports

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
Manager	Ereignismanagement-Systeme von Drittanbietern	UDP/162	SNMP-Trap
Manager	Ereignismanagement-Systeme von Drittanbietern	UDP/514	SYSLOG
Manager	E-Mail-Gateway	TCP/25	SMTP
Manager	Bedrohungs-Feed	TCP/443	SSL
Benutzer-PC	Alle Appliances	TCP/22	SSH

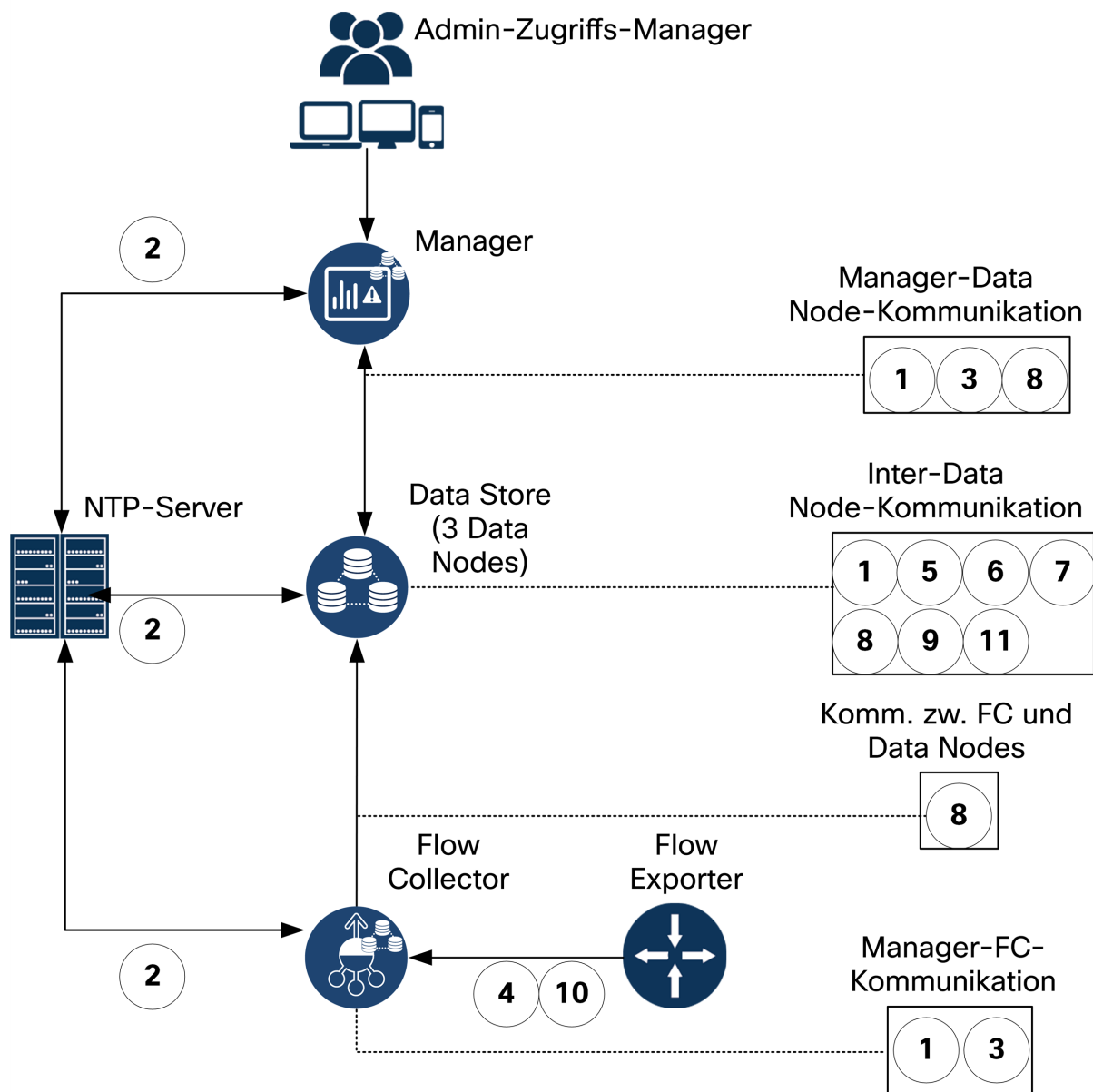
Secure Network Analytics Bereitstellungsbeispiel

Das folgende Diagramm zeigt die verschiedenen Verbindungen, die von Secure Network Analytics verwendet werden. Einige dieser Ports sind optional.



Secure Network Analytics Beispiel für eine Bereitstellung mit Data Store

Wie in der folgenden Abbildung dargestellt, können Sie Secure Network Analytics 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.



2. Installationswarnungen und Richtlinien

Installationswarnungen


Lesen Sie das Dokument [Erfüllung gesetzlicher Auflagen und Sicherheitsinformationen](#), bevor Sie Appliances der Secure Network Analytics x2xx-Serie installieren.

Beachten Sie die folgenden Warnhinweise:

Anweisung 1071 – Definition der Warnhinweise


WICHTIGE SICHERHEITSANWEISUNGEN

Dieses Warnsymbol weist auf eine Gefahr hin. Sie befinden sich möglicherweise in einer Situation, in der es zu körperlichen Verletzungen kommen kann. Machen


-  Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung von Unfällen vertraut. 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.


Anweisung 1004 – Installationsanweisungen

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

Anweisung 1005 – Leitungsschutzschalter

-  Dieses Produkt ist für Gebäude mit Kurzschlussicherung (Überstromschutz) gedacht.

Anweisung 1006 – Warnhinweis zum Chassis bei der Rackmontage und -wartung

-  Treffen Sie bei der Montage oder Wartung des Geräts in einem Rack entsprechende Vorkehrungen, um Verletzungen durch eine mögliche Instabilität des Systems zu vermeiden. Beachten Sie zu Ihrer eigenen Sicherheit die folgenden Hinweise:
- Ist das Gerät das einzige im Rack, montieren Sie es unten im Rack.

- Soll das Gerät in einem bereits teilweise gefüllten Rack montiert werden, bestücken Sie das Rack von unten nach oben, wobei die schwerste Komponente unten im Rack montiert wird.



- Soll das Gerät in einem bereits teilweise gefüllten Rack montiert werden, bestücken Sie das Rack von unten nach oben, wobei die schwerste Komponente unten im Rack montiert wird.

Anweisung 1015 – Batterieaustausch

So minimieren Sie die Brand- und Explosionsgefahr oder das Austreten von brennbaren Flüssigkeiten oder Gasen:

- Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp.



- Die Batterie darf nicht ausgebaut, zerquetscht, durchstochen oder mit scharfkantigem Werkzeug entfernt werden. Versuchen Sie nicht, die externen Kontakte kurzzuschließen, und werfen Sie die Batterie nicht ins Feuer.

- Verwenden Sie die Batterie nicht, wenn sie aufgequollen oder verformt ist.

- Lagern oder verwenden Sie die Batterie nicht bei Temperaturen über 60 °C.

- Lagern oder verwenden Sie die Batterie nicht in Umgebungen mit geringem Luftdruck unter 69,7 kPa.

Anweisung 1017 – Bereiche mit beschränktem Zutritt




Dieses Gerät ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Bereiche mit beschränktem Zutritt dürfen nur von geschulten und qualifizierten Personen betreten werden.

Anweisung 191 – Voluntary Control Council for Interference (VCCI) Warnung der Klasse A für Japan




Dies ist ein Produkt der Klasse A, das dem Standard des VCCI (Voluntary Control Council for Interference) entspricht. Wenn dieses Gerät in einer häuslichen Umgebung verwendet wird, kann es zu Funkstörungen kommen. In diesem Fall müssen Sie möglicherweise Korrekturmaßnahmen ergreifen.


Anweisung 164 – Hebeanforderung

-  Zum Anheben der schweren Teile des Produkts sind zwei Personen erforderlich. Halten Sie Ihren Rücken gerade und heben Sie aus den Beinen und nicht aus dem Rücken, um Verletzungen zu vermeiden.


Anweisung 256 – Warnung zur Klasse A für Ungarn

-  Dieses Gerät ist ein Produkt der Klasse A und sollte gemäß den ungarischen EMV-Anforderungen der Klasse A (MSZEN55022) verwendet und installiert werden. Geräte der Klasse A sind für typische kommerzielle Einrichtungen konzipiert, in denen besondere Installationsbedingungen und Schutzabstände gelten.


Anweisung 294 – Warnung zur Klasse A für Korea

-  Dies ist ein Gerät der Klasse A. Es erfüllt die Anforderungen an die elektromagnetische Verträglichkeit (EMV) für den industriellen Einsatz. Der Verkäufer und der Käufer sollten dies wissen. Wenn das Gerät nicht industriell eingesetzt werden soll und fälschlicherweise verkauft oder gekauft wurde, sollte es durch ein für den Betrieb in Wohngebieten geeignetes Gerät ersetzt werden.

Anweisung 340 – Warnung zur Klasse A für CISPR22/EN55022/CISPR32/EN55032

-  Dies ist ein Produkt der Klasse A. In einer häuslichen Umgebung kann dieses Produkt Funkinterferenzen verursachen. In diesem Fall müssen Sie ggf. geeignete Maßnahmen ergreifen.

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-Steckverbinder. Gehen Sie beim Anschluss von Kabeln vorsichtig vor.

Anweisung 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 eine/n ElektrikerIn.

Anweisung 1028 – Mehr als ein Netzteil



Dieses Gerät kann mit mehr als einem Netzteil verbunden sein. Um die Stromschlag- und Brandgefahr zu minimieren und um sicherzustellen, dass die Stromversorgung der Einheit abgeschaltet ist, müssen alle Anschlüsse entfernt werden.

Anweisung 1029 – Leere Frontplatten und Abdeckungen



Leere Frontplatten und Abdeckungen dienen drei wichtigen Funktionen: Sie minimieren die Stromschlag- und Brandgefahr, sie schirmen elektromagnetische Interferenzen (EMI) ab, die möglicherweise andere Geräte stören, und sie leiten Kühlluft durch das Chassis. Betreiben Sie das System nur, wenn alle Karten, Frontplatten, Frontabdeckungen und hinteren Abdeckungen installiert sind.

Anweisung 1030 – Installation des Geräts



Das Installieren, Ersetzen oder Warten dieses Geräts sollte ausschließlich geschultem, qualifiziertem Personal gestattet werden.

Anweisung 1032 – Anheben des Chassis



Um Verletzungen von Personen oder Schäden am Chassis zu vermeiden, dürfen Sie niemals versuchen, das Chassis mithilfe der Griffe an den Modulen (z. B. Netzteile, Lüfter oder Karten) anzuheben oder zu kippen. Diese Griffe sind nicht dafür ausgelegt, das Gewicht des Geräts zu tragen.

Anweisung 9001 – Entsorgung des Produkts

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

Anweisung 1051 – Laserstrahlung

Von getrennten Fasern oder Anschlüssen kann unsichtbare Laserstrahlung ausgehen. Blicken Sie nicht direkt in Strahlen oder optische Instrumente.

Anweisung 1055 – Laser der Klasse 1/1M

Unsichtbare Laserstrahlung ist vorhanden. Setzen Sie BenutzerInnen von Teleskopoptiken keinem Risiko aus. Dies gilt für Laserprodukte der Klasse 1/1M.

Anweisung 1008 – Laserprodukt der Klasse 1

Dieses Produkt ist ein Laserprodukt der Klasse 1.

Anweisung 1056 – Nicht abgeschlossenes Glasfaserkabel

Von nicht abgeschlossenen Faserkabeln oder Anschlüssen kann unsichtbare Laserstrahlung ausgehen. Blicken Sie nicht direkt mit optischen Instrumenten darauf. Das Betrachten des Laserausgangs mit bestimmten optischen Geräten (Lupen, Vergrößerungsgläser, Mikroskop usw.) in einem Abstand von 100 mm kann zu Augenschäden führen.

Glasfaserart und Kerndurchmesser (µm)	Wellenlänge (nm)	Maximale Leistung (mW)	Strahlabweichung (Radius)
SM 11	1200–1400	39–50	0,1–0,11
MM 62,5	1200–1400	150	0,18 NA
MM 50	1200–1400	135	0,17 NA
SM 11	1400–1600	112–145	0,11–0,13


Anweisung 1089 – Definitionen: geschulte und qualifizierte Person

Als geschulte Person wird eine Person definiert, die von einer qualifizierten Person ausgebildet und geschult wurde. Sie unternimmt die nötigen


 Vorsichtsmaßnahmen bei der Arbeit mit den Geräten.

Eine qualifizierte Person/qualifiziertes Fachpersonal ist eine Person, die geschult wurde oder über Erfahrung mit den Geräten verfügt und potenzielle Gefahren bei der Arbeit mit den Geräten kennt.


Anweisung 1090 – Installation durch eine qualifizierte Person

 Das Installieren, Ersetzen oder Warten dieses Geräts sollte ausschließlich einer qualifizierten Person gestattet werden. Siehe Anweisung 1089 für eine Definition von qualifizierten Personen.

Anweisung 1091 – Installation durch eine geschulte Person


 Das Installieren, Ersetzen oder Warten dieses Geräts sollte ausschließlich einer geschulten oder qualifizierten Person gestattet werden. Siehe Anweisung 1089 für eine Definition von geschulten oder qualifizierten Personen.

Anweisung 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 2017 – Hinweis zur Klasse A für FCC

Das Anpassen oder Verändern der Ausrüstung ohne die Genehmigung von Cisco kann dazu führen, dass die Ausrüstung nicht länger den FCC-Bestimmungen für digitale Geräte der Klasse A entspricht. Dies kann dazu führen, dass Störungen im Bereich von Radio- und TV-Kommunikationen von Ihnen selbst und auf Ihre eigenen Kosten behoben werden müssen.

 Dieses Produkt wurde getestet und entspricht Part 15 der FCC-Bestimmungen den Grenzwerten für ein digitales Gerät der Klasse A. Diese Beschränkungen wurden entwickelt, um einen umfangreichen Schutz gegen funktechnischen Störungen zu gewährleisten, wenn das Gerät in einer kommerziellen Umgebung

betrieben wird. Dieses Gerät erzeugt und nutzt Hochfrequenzenergie und kann diese ausstrahlen. Wenn das Gerät nicht ordnungsgemäß installiert ist und nicht gemäß den Anweisungen des Benutzerhandbuchs betrieben wird, kann es zu funktechnischen Störungen in der Funkkommunikation kommen. Der Betrieb dieses Geräts in einem Wohngebiet kann unter Umständen zu funktechnischen Störungen führen. In diesem Fall muss der Benutzer diese Störungen auf eigene Kosten beheben.



Anweisung 2021 – Hinweis zur Klasse A für Kanada



Dieses digitale Gerät der Klasse A erfüllt die kanadische Norm ICES-003/NMB-003.

Anweisung 7001 – ESD-Minderung



Dieses Gerät ist möglicherweise ESD-empfindlich. Verwenden Sie immer ein Antistatikarmband für Handgelenk oder Knöchel, bevor Sie das Gerät anfassen. Verbinden Sie das Geräteende des Antistatikbands mit einer unbearbeiteten Oberfläche des Geräte-Chassis oder, falls vorhanden, mit der ESD-Buchse am Gerät.

Anweisung 7003 – Anforderungen an abgeschirmte Kabel zum Schutz vor gebäudeinternem Blitzstoß



Der/die gebäudeinterne(n) Port(s) der Geräte oder Unterbaugruppen muss/müssen abgeschirmte gebäudeinterne Verkabelung/Verdrahtung verwenden, die an beiden Enden geerdet ist. Die folgenden Ports gelten bei diesem Gerät als gebäudeinterne Ports:

Anweisung 7005 – Gebäudeinterner Blitzstoß und Ausfall der AC-Stromversorgung



Der/die gebäudeinterne(n) Port(s) der Geräte oder Unterbaugruppen ist/sind ausschließlich für den Anschluss an gebäudeinterne oder nicht freiliegende Leitungen bzw. Kabel geeignet. Die gebäudeinternen Ports der Geräte oder Unterbaugruppe dürfen NICHT für mehr als 6 Meter metallisch mit Schnittstellen verbunden sein, die an das Außennetz oder dessen Verkabelung angeschlossen werden. Diese Schnittstellen sind ausschließlich für die Nutzung als gebäudeinterne Schnittstellen vorgesehen (Ports vom Typ 2, 4 oder 4a gemäß

GR-1089) und müssen von der freiliegenden Linientechnikverkabelung isoliert werden. Das Hinzufügen einer Netzwerkschutzvorrichtung liefert keinen ausreichenden Schutz, um diese Schnittstellen mechanisch mit der Verkabelung der Linientechnik zu verbinden.



Die folgenden Ports gelten bei diesen Geräten als gebäudeinterne Ports:

Installationsrichtlinien

Beachten Sie die folgenden Warnhinweise:

Anweisung 1047 – Schutz vor Überhitzung



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.

Anweisung 1019 – Primäre Ausschaltvorrichtung



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

Anweisung 1075 – 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.

Anweisung 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, den Rettungsdienst zu rufen. 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 Schaltungen 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 Eingangsstromanforderungen 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.

3. Montage Ihrer Appliances

Sie können Secure Network Analytics-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 Secure Network Analytics-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

4. Verbinden Ihrer Appliances 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.

1. Spezifikationen prüfen

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.

- **Datenblätter:** Detaillierte Informationen zu den einzelnen Appliances finden Sie in den [Secure Network Analytics-Datenblättern](#).
- **UCS-Plattform:** Alle Hardwarekomponenten der Cisco x2xx-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.
- **Manager 2210:** Wenn Sie einen Data Store bereitstellen, können Sie einen Manager 2210 mit einer 10-Gbit/s-SFP+-DAC-Schnittstelle als eth0 für erhöhten Durchsatz konfigurieren. Wenn Sie keinen Data Store einsetzen, können Sie nur die 100-Mbit/s-/1-Gbit/s-/10-Gbit/s-Kupferschnittstelle als eth0 konfigurieren.
- **Flow Collector 4210:** Wenn Sie einen Data Store bereitstellen, können Sie einen Flow Collector 4210 mit einer 10-Gbit/s-SFP+-DAC-Schnittstelle als eth0 für erhöhten Durchsatz konfigurieren. Wenn Sie keinen Data Store einsetzen, können Sie nur die 100-Mbit/s-/1-Gbit/s-/10-Gbit/s-Kupferschnittstelle als eth0 konfigurieren.
- **Flow Collector 5210:** Der Flow Collector 5210 besteht aus zwei miteinander verbundenen Servern (Datenbank und Engine), die 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.
- Wenn Sie [Ihr System konfigurieren](#), stellen Sie sicher, dass Sie die Datenbank und die Engine in der im [Systemkonfigurationshandbuch angegebenen Reihenfolge konfigurieren](#).



Aktualisieren Sie das Appliance-BIOS nicht, da dies zu Problemen mit der Appliance-Funktionalität führen kann.

2. Verbinden Ihrer Appliance mit dem Netzwerk

So verbinden Sie Ihre Appliance mit Ihrem Netzwerk:

1. Schließen Sie ein Ethernetkabel an den Management-Port auf der Rückseite der Appliance an.
2. Schließen Sie mindestens einen Monitoring-Port für Flow Sensoren und UDP Directors an.
 - **UDP Director High Availability:** Verbinden Sie 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.
 - **Ethernet-Label:** Notieren Sie das Ethernet-Label (eth2, eth3 usw.) für jeden Port. Diese Labels entsprechen den Netzwerkschnittstellen (eth2, eth3 usw.), die in der Systemkonfiguration verwendet werden.
3. Verbinden Sie das jeweils andere Ende der Ethernetkabel mit dem Switch Ihres Netzwerks.
4. Verbinden Sie die Netzkabel mit dem Netzteil. Einige Appliances verfügen über zwei Stromanschlüsse: Netzteil 1 und Netzteil 2.

5. Verbinden mit Ihrer Appliance

In diesem Abschnitt wird beschrieben, wie Sie eine Verbindung zur Appliance für die Systemkonfiguration herstellen.

Wählen Sie Ihr Verbindungsverfahren aus:

- **Anschluss einer Tastatur und eines Monitors**
- **Anschluss eines seriellen Kabels oder einer seriellen Konsole**
- **Verbinden mit CIMC (für Remote-Zugriff erforderlich)**
Nutzen Sie dieses Verbindungsverfahren, um eine Verbindung mit der Appliance für den Remote-Zugriff herzustellen.

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 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. Gehen Sie zu **6. Konfigurieren des Secure Network Analytics-Systems**.

Anschluss eines seriellen Kabels oder einer seriellen Konsole

Sie können die Appliance mit einem seriellen Kabel oder einer seriellen Konsole, wie z. B. einem Laptop mit Terminal-Emulator, verbinden. Wir verwenden in den Anweisungen einen Laptop als Beispiel.

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 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. Gehen Sie zu **6. Konfigurieren des Secure Network Analytics-Systems**.

Verbinden mit CIMC (für Remote-Zugriff erforderlich)

Der Cisco Integrated Management Controller (CIMC) ermöglicht den Zugriff auf die Serverkonfiguration und eine virtuelle Serverkonsole sowie das Monitoring des Hardwarezustands. Sie verwenden den CIMC auch in der Secure Network Analytics-Systemkonfiguration.

1. Befolgen Sie die Anweisungen im [Konfigurationsleitfaden für die GUI des Integrated Management Controllers der Cisco UCS C-Series](#).
2. Melden Sie sich bei CIMC als Administrator an und geben Sie **password** in das Kennwortfeld ein.
3. Ändern Sie das Standardkennwort, um die Sicherheit Ihres Netzwerks zu gewährleisten.
4. Gehen Sie zu **6. Konfigurieren des Secure Network Analytics-Systems**.

6. Konfigurieren des Secure Network Analytics-Systems

Wenn Sie die Installation Ihrer Appliances der Virtual Edition und/oder Ihrer Hardware-Appliances abgeschlossen haben, können Sie Secure Network Analytics in einem gemanagten System konfigurieren.

Um Secure Network Analytics zu konfigurieren, befolgen Sie die Anweisungen im [Secure Network Analytics-Systemkonfigurationshandbuch v7.5.0](#). Dieser Schritt ist entscheidend für die erfolgreiche Konfiguration und Kommunikation Ihres Systems.

Stellen Sie sicher, dass Sie Ihre Appliances in der im Systemkonfigurationshandbuch angegebenen Reihenfolge konfigurieren.

Systemkonfigurationsanforderungen

Stellen Sie sicher, dass Sie über [CIMC](#) Zugriff auf die Appliance-Konsole haben.

Verwenden Sie die folgende Tabelle, um die erforderlichen Informationen für jede Appliance vorzubereiten.

Konfigurationsanforderungen	Details	Appliance
IP-Adresse	Weisen Sie dem <code>eth0</code> -Management-Port eine routbare IP-Adresse zu.	
Netmask (Netzmaske)		
Gateway		
Hostname	Für jede Appliance ist ein eindeutiger Hostname erforderlich. Wir können keine Appliance mit demselben Hostnamen wie eine andere Appliance konfigurieren. Stellen Sie außerdem sicher, dass jeder Hostname der Appliance die Internetstandardanforderungen für Internethosts erfüllt.	

Domänenname	Für jede Appliance ist ein vollständig qualifizierter Domänenname erforderlich. Wir können keine Appliance mit einer leeren Domäne installieren.	
DNS-Server	Interner DNS-Server zur Namensauflösung	
NTP-Server	<p>Interner Zeitserver für die Synchronisierung zwischen Servern. Für jede Appliance ist mindestens 1 NTP-Server erforderlich.</p> <p>Entfernen Sie den NTP-Server 130.126.24.53, wenn er in Ihrer Serverliste aufgeführt ist. Dieser Server ist bekanntermaßen problematisch und wird in unserer Standardliste von NTP-Servern nicht mehr unterstützt.</p>	
Mail-Relay-Server	SMTP-Mail-Server zum Senden von Warnungen und Benachrichtigungen	
Flow Collector Export-Port	Nur für Flow Collectors erforderlich. Netflow-Standard: 2055	
Nicht routbare IP-Adresse in einem privaten LAN oder VLAN (für die Kommunikation zwischen Data Nodes)	<p>Nur für Data Nodes erforderlich.</p> <ul style="list-style-type: none"> Hardware eth2 oder Bündelung von eth2 und eth3. Die Erstellung eines LACP eth2/eth3-Port-Channels für bis zu 20G-Durchsatz ermöglicht eine schnellere Kommunikation der Data Nodes untereinander und ein schnelleres Hinzufügen oder Ersetzen von Data Nodes zum 	

	<p>Data Store. Beachten Sie, dass LACP-Port-Bonding die einzige verfügbare Bonding-Option für Hardware-Data Nodes ist.</p> <ul style="list-style-type: none">• Virtueller eth1 <p>IP-Adresse: Sie können die angegebene IP-Adresse verwenden oder einen Wert eingeben, der die folgenden Anforderungen für die Kommunikation zwischen Data Nodes erfüllt.</p> <ul style="list-style-type: none">• Nicht routbare IP-Adresse aus dem CIDR-Block 169.254.42.0/24, zwischen 169.254.42.2 und 169.254.42.254.• Ersten drei Oktette: 169.254.42• Subnetz: /24• Sequenziell: Um die Wartung zu erleichtern, wählen Sie aufeinanderfolgende IP-Adressen (z. B. 169.254.42.10, 169.254.42.11 und 169.254.42.12). <p>Netzmaske</p> <p>Die Netzmaske ist fest auf 255.255.255.0 codiert und kann nicht geändert werden.</p>	
--	---	--

eth0-Verbindungsport für Hardware	Erforderlich nur für Secure Network Analytics mit Data Store-Hardware-Appliances: <ul style="list-style-type: none">• Manager• Flow Collector• Data Nodes eth0-Portoptionen für Hardware-Verbindungen: <ul style="list-style-type: none">• SFP+	
-----------------------------------	--	--

Support kontaktieren

Wenn Sie technischen Support benötigen, haben Sie folgende Möglichkeiten:

- Wenden Sie sich an Ihren lokalen Cisco Partner
- Wenden Sie sich an den technischen Support von Cisco
- Erstellen Sie online ein Ticket: <http://www.cisco.com/c/en/us/support/index.html>
- Erstellen Sie ein Ticket per E-Mail: tac@cisco.com
- Rufen Sie uns an: 1-800-553-2447 (USA)
- Weltweite Supportnummern finden Sie unter:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Änderungsverlauf

Dokumentversion	Veröffentlichungsdatum	Beschreibung
1_0	15. Dezember 2023	Erste Version

Copyright-Informationen

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter folgender URL: <https://www.cisco.com/go/trademarks>. Die genannten Handelsmarken von Drittanbietern sind Eigentum der jeweiligen Inhaber. Die Verwendung des Worts "Partner" deutet keine Handelsbeziehung zwischen Cisco und anderen Unternehmen an. (1721R)