

Cisco Secure Network Analytics

Virtual Edition Appliance Installation Guide 7.4.2



Table of Contents

Introduction	6
Overview	6
Audience	6
Installing Appliances and Configuring Your System	6
Related Information	6
Terminology	7
Abbreviations	7
Secure Network Analytics without Data Store	9
Secure Network Analytics with Data Store	10
Queries	11
Data Store Storage and Fault Tolerance	11
Telemetry Storage Example	12
General Deployment Requirements	13
Installation Methods	13
Compatibility	14
General Requirements for All Appliances	14
VMware	14
KVM	15
Downloading Software	15
TLS	15
Third Party Applications	16
Browsers	16
Host Name	16
Domain Name	16
NTP Server	16
Time Zone	16
Standard Appliance Requirements (without Data Store)	17
Manager and Flow Collector Deployment Requirements	17

Data Store Deployment Requirements	18
Appliance Requirements (with Data Store)	18
Manager and Flow Collector Deployment Requirements	18
Data Node Deployment Requirements	18
Multi-Data Node Deployment	19
Supported Hardware Metrics (with Analytics enabled)	20
Supported Hardware Metrics (without Analytics enabled)	20
Single Data Node Deployment	20
Data Node Configuration Requirements	21
Networking and Switching Considerations	21
Virtual Switch Example	23
Data Store Placement Considerations	23
Analytics Deployment Requirements	24
Resource Requirements	25
CPU Settings Calculation	26
Manager Virtual Edition	27
Manager	27
Flow Collector Virtual Edition	28
Flow Collector without Data Store	28
Flow Collector with Data Store	29
Data Node Virtual Edition	30
Data Store with a Single Virtual Data Node	30
Data Store with 3 Virtual Data Nodes	31
Flow Sensor Virtual Edition	32
Flow Sensor Virtual Edition Network Environments	34
Flow Sensor Virtual Edition Traffic	34
UDP Director Virtual Edition	35
Calculating Flows Per Second (Optional)	36
Calculating Flows Per Second for Flow Collector Storage (Deployments without Data Store)	36

Calculating Flows Per Second for Data Node Storage	36
1. Configuring Your Firewall for Communications	38
Open Ports (All Appliances)	38
Additional Open Ports for Data Nodes	38
Communication Ports and Protocols	39
Additional Open Ports for Data Store	41
Optional Communication Ports	42
Secure Network Analytics Deployment Example	43
Secure Network Analytics Deployment with Data Store Example	44
2. Downloading Virtual Edition Installation Files	45
Installation Files	45
1. Log in to Cisco Software Central	45
2. Download Files	46
3a. Installing a Virtual Appliance using VMware vCenter (ISO)	47
Overview	47
Before You Begin	47
Installing a Virtual Appliance Using vCenter (ISO)	48
Data Nodes	48
Flow Sensors	48
All Other Appliances	48
1. Configuring an Isolated LAN for inter-Data Node Communications	49
Configuring a vSphere Standard Switch	49
Configuring a vSphere Distributed Switch	49
2. Configuring the Flow Sensor to Monitor Traffic	49
Monitoring External Traffic with PCI Pass-Through	50
Monitoring a vSwitch with Multiple Hosts	51
Configuration Requirements	51
Monitoring a vSwitch with a Single Host	54
Configuration Requirements	54
Configure the Port Group to Promiscuous Mode	54

3. Installing the Virtual Appliance	57
4. Defining Additional Monitoring Ports (Flow Sensors only)	64
3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)	67
Overview	67
Before You Begin	67
Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)	68
Process Overview	68
Data Nodes	68
1. Logging in to the VMware Web Client	68
2. Booting from the ISO	71
3c. Installing a Virtual Appliance on a KVM Host (ISO)	73
Overview	73
Before You Begin	73
Installing a Virtual Appliance on a KVM Host (ISO)	74
Process Overview	74
Configuring an Isolated LAN for Data Nodes	74
1. Installing a Virtual Appliance on a KVM Host	74
Monitoring Traffic	74
Configuration Requirements	74
Installing a Virtual Appliance on a KVM Host	75
2. Adding NIC (Data Node, Flow Sensor) and Promiscuous Port Monitoring on an Open vSwitch (Flow Sensors Only)	81
4. Configuring Your Secure Network Analytics System	84
System Configuration Requirements	84
Contacting Support	87
Change History	89

Introduction

Overview

Use this guide to install the following Cisco Secure Network Analytics (formerly Stealthwatch) Virtual Edition appliances:

- Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console) Virtual Edition
- Cisco Secure Network Analytics Data Store Virtual Edition
- Cisco Secure Network Analytics Flow Collector Virtual Edition
- Cisco Secure Network Analytics Flow Sensor Virtual Edition
- Cisco Secure Network Analytics UDP Director Virtual Edition

Audience

The intended audience for this guide includes network administrators and other personnel who are responsible for installing and configuring Secure Network Analytics products.

If you are configuring virtual appliances, we assume you have basic familiarity with VMware or KVM.

If you prefer to work with a professional installer, please contact your local Cisco Partner or [Cisco Support](#).

Installing Appliances and Configuring Your System

Please note the overall workflow for installing and configuring Secure Network Analytics.

1. **Install Appliances:** Install your Secure Network Analytics Virtual Edition appliances using this installation guide. To install hardware (physical) appliances, follow the instructions in the [x2xx Series Hardware Appliance Installation Guide](#) or the [x3xx Series Hardware Appliance Installation Guide](#).
2. **Configure Secure Network Analytics:** After you install hardware and virtual appliances, you are ready to configure Secure Network Analytics into a managed system. Follow the instructions in the [Secure Network Analytics System Configuration Guide v7.4.2](#).

Related Information

For more information about Secure Network Analytics, refer to the following resources:

- **Overview:**

- <https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>

- **Data Store Design Guide:**

- <https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf>

Terminology

This guide uses the term “**appliance**” for any Secure Network Analytics product, including virtual products such as the Flow Sensor Virtual Edition (VE).

A “**cluster**” is your group of Secure Network Analytics appliances that are managed by the Manager.

Abbreviations

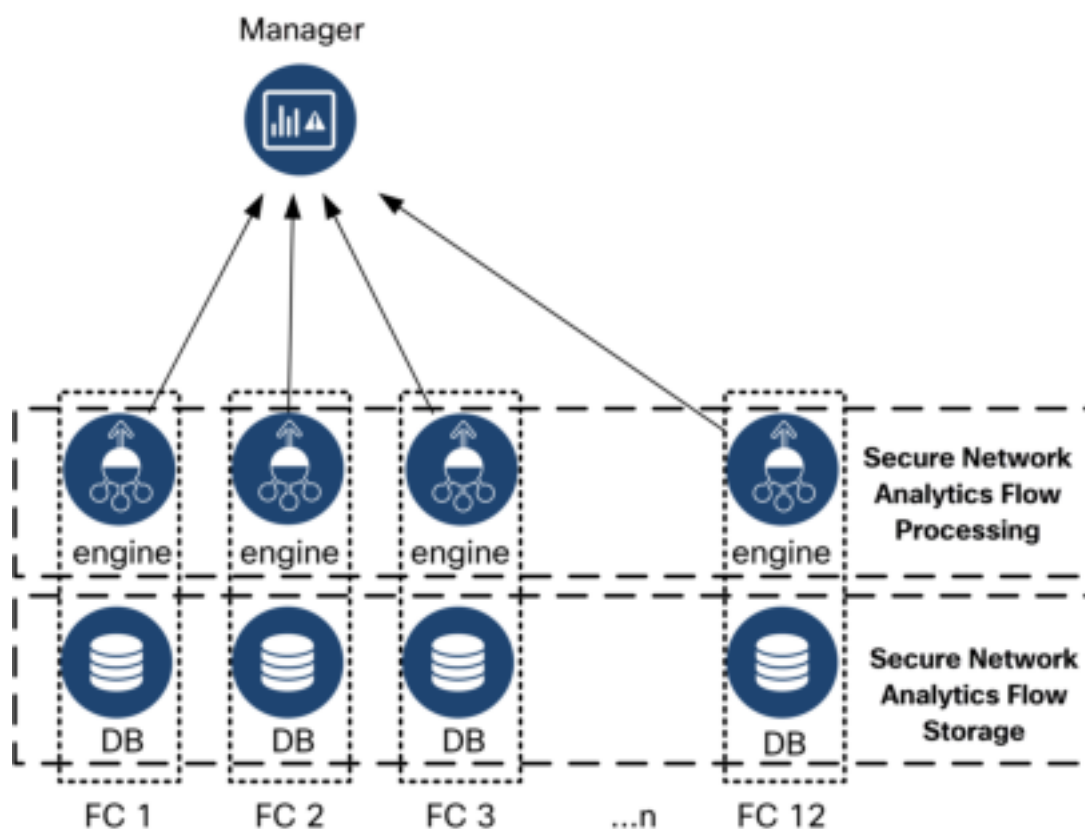
The following abbreviations may appear in this guide:

Abbreviations	Definition
DNS	Domain Name System (Service or Server)
dvPort	Distributed Virtual Port
ESX	Enterprise Server X
GB	Gigabyte
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Standards Organization
IT	Information Technology
KVM	Kernel-based Virtual Machine
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
TB	Terabyte

Abbreviations	Definition
UUID	Universally Unique Identifier
VDS	vNetwork Distributed Switch
VLAN	Virtual Local Area Network
VM	Virtual Machine

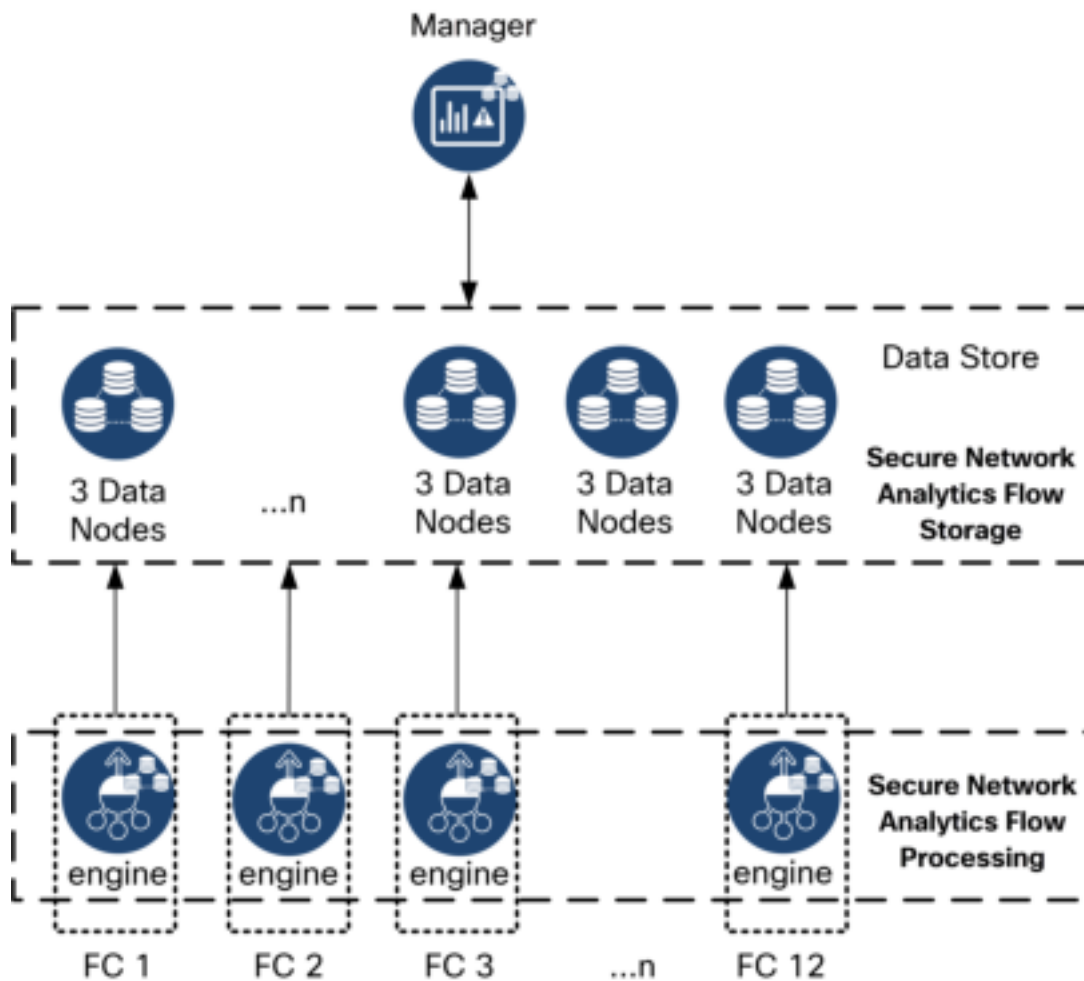
Secure Network Analytics without Data Store

In a Secure Network Analytics deployment without a Data Store, one or more Flow Collectors ingests and deduplicates data, performs analysis, and reports data and results directly to the Manager. To resolve user-submitted queries, including graphs and charts, the Manager queries all of the managed Flow Collectors. Each Flow Collector returns matching results to the Manager. The Manager collates the information from the different result sets, then generates a graph or chart displaying the results. In this deployment, each Flow Collector stores data on a local database. See the following diagram for an example.



Secure Network Analytics with Data Store

In a Secure Network Analytics deployment with a Data Store, the Data Store cluster sits between your Manager and Flow Collectors. One or more Flow Collectors ingest and deduplicate flows, perform analysis, and reports data and results directly to the Data Store, distributing it roughly equally to all of the Data Nodes. The Data Store facilitates data storage, keeps all of your traffic in that centralized location as opposed to spread across multiple Flow Collectors, and it offers greater storage capacity than multiple Flow Collectors. See the following diagram for an example.



The Data Store provides a central repository to store your network's telemetry, collected by your Flow Collectors. The Data Store is comprised of a cluster of Data Nodes, each containing a portion of your data, and a backup of a separate Data Node's data. Because all of your data is in one centralized database, as opposed to spread across multiple Flow Collectors, your Manager can retrieve query results from the Data Store more quickly than if it queried all of your Flow Collectors separately. The Data Store cluster provides

improved fault tolerance, improved query response, and quicker graph and chart population.

Queries

To resolve user-submitted queries, including graphs and charts, the Manager queries the Data Store. The Data Store finds matching results in the columns relevant to the query, then retrieves the matching rows and returns the query results to the Manager. The Manager generates the graph or chart without needing to collate multiple result sets from multiple Flow Collectors. This reduces the cost of querying, as compared to querying multiple Flow Collectors, and improves query performance.

Data Store Storage and Fault Tolerance

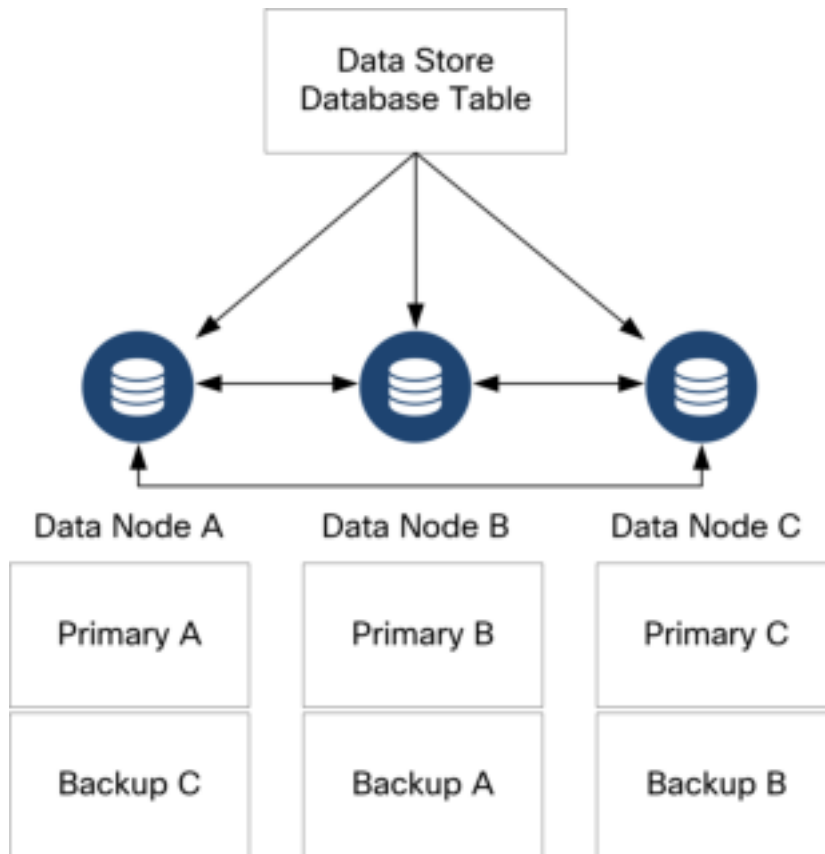
The Data Store collects data from Flow Collectors and distributes it equally across Data Nodes within the cluster. Each Data Node, in addition to storing a portion of your overall telemetry, also stores a backup of another Data Node's telemetry. Storing data in this fashion:

- helps with load balancing
- distributes processing across each node
- ensures all data ingested into the Data Store has a backup for fault tolerance
- allows for increasing the number of Data Nodes to improve overall storage and query performance

If your Data Store has 3 or more Data Nodes, and a Data Node goes down, as long as the Data Node containing its backup is still available, and at least half of your total number of Data Nodes are still up, the overall Data Store remains up. This allows you time to repair the downed connection or faulty hardware. After you replace the faulty Data Node, the Data Store restores that node's data from the existing backup stored on the adjacent Data Node, and creates a backup of data on that Data Node.

Telemetry Storage Example

See the following diagram for an example of how 3 Data Nodes store telemetry:



General Deployment Requirements

Before you begin, review this guide to understand the process as well as the preparation, time, and resources you'll need to plan for the installation.

Installation Methods

You can use a VMware environment or KVM (Kernel-based Virtual Machine) for the virtual appliance installation.



Before you start the installation, review the [Compatibility](#) information and [Resource Requirements](#) shown in the following sections.

Method	Installation Instructions (for reference)	Installation File	Details
VMware vCenter	3a. Installing a Virtual Appliance using VMware vCenter (ISO)	ISO	Installing your virtual appliances using VMware vCenter.
VMware ESXi Stand-Alone Server	3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)	ISO	Installing your virtual appliances on an ESXi stand-alone host server.
KVM and Virtual Machine Manager	3c. Installing a Virtual Appliance on a KVM Host (ISO)	ISO	Installing your virtual appliances using KVM and Virtual Machine Manager.

Compatibility

Whether you plan to install your virtual appliances in a VMware environment or KVM (Kernel-based Virtual Machine), make sure you review the following compatibility information:

General Requirements for All Appliances

Requirement	Description
Dedicated Resources	All appliances require the allocation of dedicated resources and cannot be shared with other appliances or hosts.
No Live Migration	Appliances do not support vMotion due to the possibility of corruption.
Network Adapter	All appliances require at least 1 network adapter. Flow Sensors can be configured with additional adapters to support additional throughput. Data Nodes require a second network adapter for communication with other Data Nodes as part of the Data Store.
Storage Controller	When configuring the ISO in VMware, select the <code>LSI Logic SAS SCSI Controller</code> type.
Storage Provisioning	Assign Thick Provisioned Lazy Zeroed storage provisioning when deploying virtual appliances.

VMware

- **Compatibility:** VMware 7.0 or 8.0.
- **Operating System:** Debian 11 64-bit
- **Network Adapter:** The VMXNET3 Adapter Type is recommended for best performance.
- **ISO Deployment:** Secure Network Analytics v7.4.2 is compatible with VMware 7.0 and 8.0. We do not support VMware 6.0, 6.5, or 6.7 with Secure Network Analytics v7.4.x. For more information, refer to VMware documentation for vSphere 6.0, 6.5, and 6.7 End of General Support.

- **Live migration:** We do not support host to host live migration (for example, with vMotion).
- **Snapshots:** Virtual machine snapshots are not supported.



Do not install VMware Tools on a Secure Network Analytics virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

KVM

- **Compatibility:** You can use any compatible Linux distribution.
- **KVM Host Versions:** There are several methods used to install a virtual machine on a KVM host. We tested KVM and validated performance using the following components:
 - libvirt 2.10 – 7.1.0
 - qemu-KVM 2.6.1 – 5.2.0
 - Open vSwitch 2.6.x – 2.15.x****
 - Linux Kernel 4.4.x, and some 5.10.x
- **Operating System:** Debian 11 64-bit.
- **Virtualization Host:** For minimum requirements and best performance, review the [Resource Requirements](#) section and see the hardware specification sheet for your appliance at [Cisco.com](https://www.cisco.com).



The system performance is determined by the host environment. Your performance may vary.

Downloading Software

Use Cisco Software Central to download virtual appliance (VE) installation files, patches, and software update files. Log in to your Cisco Smart Account at <https://software.cisco.com> or contact your administrator. Refer to [2. Downloading Virtual Edition Installation Files](#) for instructions.

TLS

Secure Network Analytics requires v1.2.

Third Party Applications

Secure Network Analytics does not support installing third party applications on appliances.

Browsers

- **Compatible Browsers:** Secure Network Analytics supports the latest version of Chrome, Firefox, and Edge.
- **Microsoft Edge:** There may be a file size limitation with Microsoft Edge. We do not recommend using Microsoft Edge to install the Virtual Edition ISO files.

Host Name

A unique host name is required for each appliance. We cannot configure an appliance with the same host name as another appliance. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.

Domain Name

A fully qualified domain name is required for each appliance. We cannot install an appliance with an empty domain.

NTP Server

- **Configuration:** At least 1 NTP server is required for each appliance.
- **Problematic NTP:** Remove the 130.126.24.53 NTP server if it is in your list of servers. This server is known to be problematic and it is no longer supported in our default list of NTP servers.

Time Zone

All Secure Network Analytics appliances use Coordinated Universal Time (UTC).

- **Virtual Host Server:** Make sure your virtual host server is set to the correct time.



Make sure the time setting on the virtual host server (where you will be installing the virtual appliances) is set to the correct time. Otherwise, the appliances may not be able to boot up.

Standard Appliance Requirements (without Data Store)

If you are installing Secure Network Analytics without a Data Store, install the following appliances:

Appliance	Requirement
Manager	• Minimum of 1 Manager
Flow Collector	• Minimum of 1 Flow Collector
UDP Director	Optional
Flow Sensor	Optional

To review appliance installation requirements for Secure Network Analytics with a Data Store, refer to [Data Store Deployment Requirements](#).

Manager and Flow Collector Deployment Requirements

For each Manager and Flow Collector that you deploy, assign a routable IP address to the `eth0` management port.

Data Store Deployment Requirements

To deploy Secure Network Analytics with a Data Store, review the following requirements and recommendations for your deployment.

Appliance Requirements (with Data Store)

The following table provides an overview for the appliances required to deploy Secure Network Analytics with Data Store.

Appliance	Requirement
Manager	• Minimum of 1 Manager
Data Store	• Minimum of 1 or 3 Data Nodes • Additional sets of 3 Data Nodes to expand the Data Store, maximum of 36 Data Nodes • Deploying only 2 Data Nodes in a cluster is not supported.
Flow Collector	• Minimum of 1 Flow Collector
Flow Sensor	Optional

Manager and Flow Collector Deployment Requirements

For each Manager and Flow Collector that you deploy, assign a routable IP address to the `eth0` management port.

Data Node Deployment Requirements

Each Data Store is comprised of Data Nodes.

- **Virtual Edition:** When you download a virtual Data Store, you can deploy 1, 3, or more Data Nodes Virtual Edition (in sets of 3).
- **Hardware:** You can also install hardware Data Nodes. A DN 6300 Data Store provides a single Data Node hardware chassis.



Make sure your Data Nodes are all hardware or all Virtual Edition. Mixing hardware and virtual Data Nodes is not supported and hardware must be from the same hardware generation (all DS 6200 or all DN 6300).

Multi-Data Node Deployment

A multi-Data Node deployment provides maximum performance results.

Note the following:

- **Sets of Three:** The Data Nodes can be clustered as part of your Data Store in sets of 3, from a minimum of 3 to a maximum of 36. Deploying only 2 Data Nodes in a cluster is not supported.
- **All Hardware or All Virtual:** Make sure your Data Nodes are all hardware (of the same generation) or all Virtual Edition. Mixing hardware and virtual Data Nodes or mixing Data Store 6200 and Data Node 6300 Data Nodes is not supported.
- **Data Node Profile Size:** If you deploy Virtual Edition Data Nodes, make sure they are all the same profile size so they have the same RAM, CPU, and disk space. For details, refer to [Data Node Virtual Edition](#) in the Resource Requirements section.

Supported Hardware Metrics (with Analytics enabled)

Number of Nodes	Flows Per Second	Unique Internal Hosts
1	600,000	1.3 million
3 and above	600,000	1.3 million
3 and above	850,000	700,000



These recommendations consider only telemetry. Your performance may vary depending on additional factors, including host count, Flow Sensor use, traffic profiles, and other network characteristics. Contact [Cisco Support](#) for assistance with sizing.

Supported Hardware Metrics (without Analytics enabled)

Number of Nodes	Flows Per Second	Unique Internal Hosts
1	Up to 1 million	Up to 33 million
3 and above	Up to 3 million	Up to 33 million



These numbers are generated in our test environments using average customer data with 1.3 million unique hosts. There are several factors that may affect your specific performance, such as number of hosts, average flow size, and more. Contact [Cisco Support](#) for assistance with sizing.

Single Data Node Deployment

If you choose to deploy a single (1) Data Node:

- **Flow Collectors:** A maximum of 4 Flow Collectors are supported.
- **Adding Data Nodes:** If you deploy only one Data Node, you can add Data Nodes to your deployment in the future. Refer to [Multi-Data Node Deployment](#) for details.



These recommendations consider only telemetry. Your performance may vary depending on additional factors, including host count, Flow Sensor use, traffic profiles, and other network characteristics. Contact [Cisco Support](#) for assistance with sizing.



Currently, the Data Store does not support deploying spare Data Nodes as automatic replacements if a primary Data Node goes down. Contact [Cisco Support](#) for guidance.

Data Node Configuration Requirements

To deploy a Data Store, assign the following to each Data Node. The information you prepare will be configured in First Time Setup using the [System Configuration Guide](#).

- **Routable IP Address (eth0):** For management, ingest, and query communications with your Secure Network Analytics appliances.
- **Inter-Data Node Communications:** Configure a non-routable IP address from the 169.254.42.0/24 CIDR block within a private LAN or VLAN to be used for inter-Data Node communication.

For improved throughput performance, connect the port channel containing `eth2` and `eth3`. Ensure that each Data Node can reach every other Data Node through a virtual switch or isolated network. As part of the Data Store, your Data Nodes communicate between and among each other.

- **Network Connections:** You need two network connections, one for the management, ingest, and query communications, and one for the inter-Data Node communications.

Networking and Switching Considerations

The following table provides an overview for the networking and switching considerations for deploying Secure Network Analytics with a Data Store.

Network Consideration	Description
Inter-Data Node Communications	• Configure an isolated LAN with a virtual switch so that the Data Nodes can communicate with each other. • Establish a recommended round-trip time (RTT) latency of under 200 microseconds between and among Data Nodes

	• Keep clock skew at 1 second or lower between and among your Data Nodes. • Establish a recommended throughput of 6.4Gbps or greater (10 Gbps full duplex switched connection) between and among your Data Nodes.
Data Node Switching	• Data Nodes require their own Layer 2 VLAN to allow inter-Data Node communication. Virtual Data Nodes can be connected to an isolated network, depending on how you deploy your Data Nodes VE.
Secure Network Analytics Appliance Communications	• Manager and Flow Collectors must be able to reach all Data Nodes • Data Nodes must be able to reach Manager, all Flow Collectors, and each Data Node

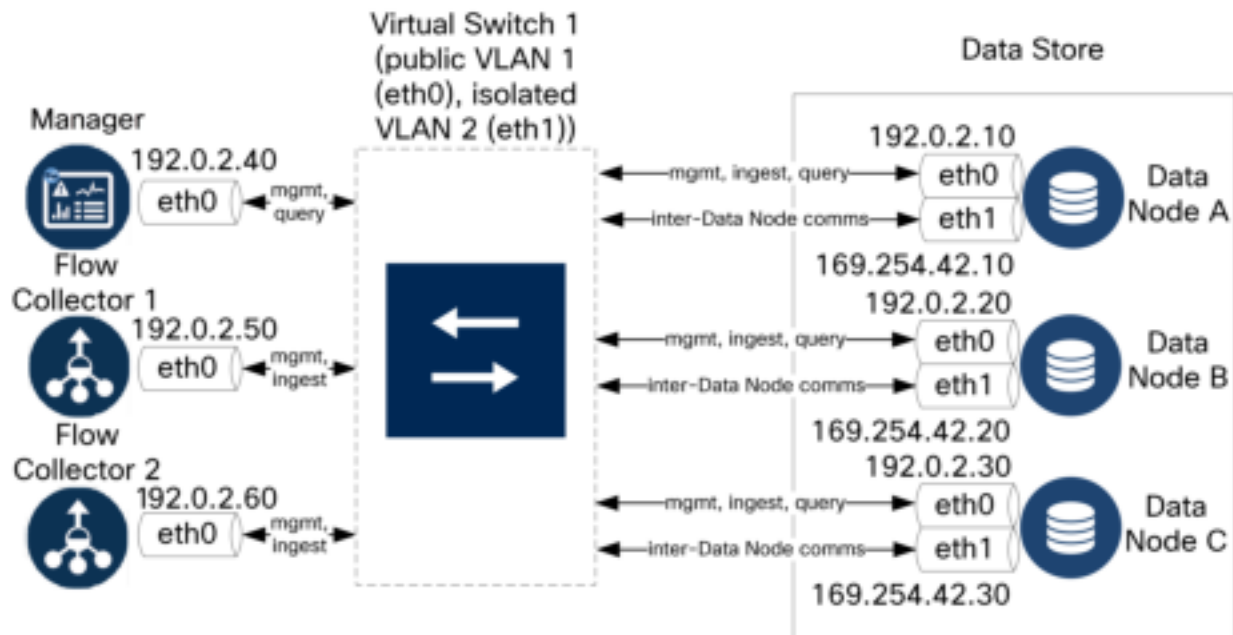


Currently, the Data Store does not support deploying spare Data Nodes as automatic replacements if a primary Data Node goes down. Please contact [Cisco Support](#) for guidance.

Virtual Switch Example

To enable inter-Data Node communications over `eth1`, configure a virtual switch with an isolated LAN or VLAN for inter-Data Node communications. Dedicate the virtual switch to inter-Data Node communications.

Also configure a public LAN or VLAN for Data Nodes `eth0` communications with the Manager and Flow Collectors. See the following diagram for an example:



The Data Store cluster requires a continuous heartbeat between nodes within the isolated VLAN. Without this heartbeat, Data Nodes may potentially go offline, which increases the risk of the Data Store going down.



Contact Cisco Professional Services for assistance with planning your deployment.

Data Store Placement Considerations

Place each Data Node so that it can communicate with all of your Flow Collectors, your Manager, and every other Data Node. For best performance, colocate your Data Nodes and Flow Collectors to minimize communication latency, and colocate Data Nodes and Manager for optimum query performance.

- **Firewall:** We highly recommend placing the Data Nodes within your firewall, such as within a NOC.

- **Physical Host/Hypervisor:** For ease of configuration, deploy all of your Data Nodes Virtual Edition to the same physical host/hypervisor, to simplify configuration of inter-Data Node configuration over an isolated LAN.
- **Power:** If the Data Store goes down due to loss of power or hardware failure, you run an increased risk of data corruption and data loss. Install your Data Nodes with constant uptime in mind.



If a Data Node loses power unexpectedly, and you reboot the appliance, the database instance on that Data Node may not automatically restart. Refer to the [System Configuration Guide](#) for troubleshooting and manually restarting the database.

Analytics Deployment Requirements

Secure Network Analytics uses dynamic entity modeling to track the state of your network. In the context of Secure Network Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they perform on your network. For more information, refer to the [Analytics: Detections, Alerts, and Observations Guide](#).

In order to enable Analytics, your deployment must be configured

- on a Virtual or a Hardware Data Store deployment with any number of Flow Collectors.
- with only 1 Secure Network Analytics Data Store domain.

Resource Requirements

This section provides the resource requirements for the virtual appliances.

Use the tables provided in this section to record settings you will need to install and configure the Secure Network Analytics Virtual Edition appliances.

- **Manager Virtual Edition**
- **Flow Collector Virtual Edition**
- **Data Node Virtual Edition**
- **Flow Sensor Virtual Edition**
- **UDP Director Virtual Edition**
- **Calculating Flows Per Second (Optional)**

Make sure you reserve the required resources for your system. This step is critical for system performance.

 If you choose to deploy Cisco Secure Network Analytics appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.



The gigabyte or GB references in the following tables is defined as follows: A unit of information equal to 2 raised to the 30th power, or strictly 1,073,741,824 bytes.

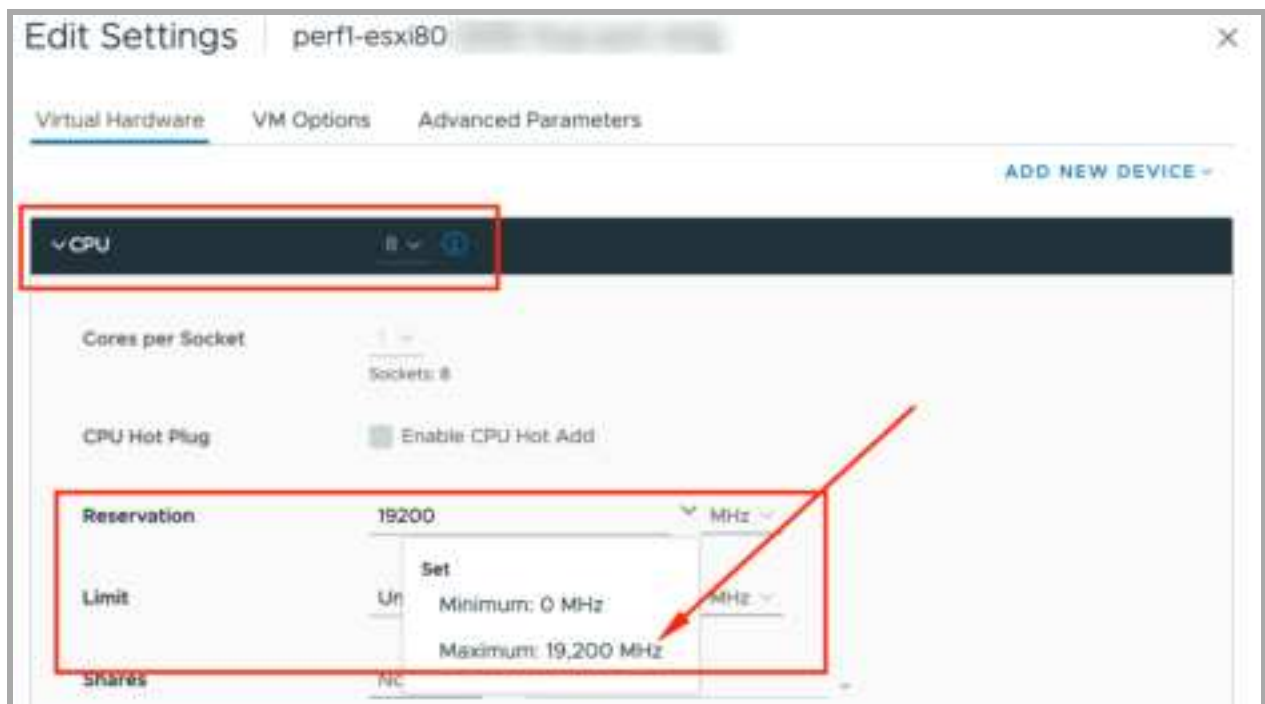
CPU Settings Calculation

For maximum performance when reserving CPUs on ESXi hosts, ensure that in your CPU Settings, the Reservation setting for CPU frequency uses the following calculation:

<Recommended number of CPUs> * <Core Frequency> = <Frequency Reservation>

You can find the core frequency (Processor Type) of your CPU under the “Host Details” section of your hypervisor.

In the example below, you would multiply 8 CPUs by the core frequency, which in this case is 2,400MHz (or 2.4 GHz). This gives you a number of 19200 MHz, which you will use for your frequency reservation.



For more information, refer to [3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server \(ISO\)](#).

Manager Virtual Edition

To determine the minimum resource allocations for the Manager Virtual Edition, determine the number of concurrent users expected to log in to the Manager. Refer to the following specifications to determine your resource allocations:

Manager

Concurrent Users*	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage	Flows per second	Internal Hosts
up to 9	6	40 GB	200 GB	Up to 100,000	100,000
over 10	12	70 GB	480 GB	Over 100,000	250,000

*Concurrent users include scheduled reports and people using the Manager client at the same time.

Flow Collector Virtual Edition

To determine your resource requirements for the Flow Collector Virtual Edition, make sure you calculate the flows per second expected on the network and the number of exporters and hosts it is expected to monitor. Refer to the [Calculating Flows Per Second](#) section for details.

Also, the minimum storage space may increase based on your FPS calculation and your retention requirements.

Because the Data Nodes within a Data Store will store flows instead of the Flow Collectors, make sure you refer to the specifications for your planned deployment (without Data Store or with Data Store).

Flow Collector without Data Store

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Data Storage for 30 Days	Interfaces	Exporters	Internal Hosts
Up to 10,000	2	24 GB	600 GB	Up to 65535	Up to 1024	25,000
Up to 30,000	6	32 GB	900 GB	Up to 65535	Up to 1024	100,000
Up to 60,000	8	64 GB	1.8 TB	Up to 65535	Up to 2048	250,000
Up to 120,000	12	128 GB	3.6 TB	Up to 65535	Up to 4096	over 250,000

Flow Collector with Data Store

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage	Interfaces	Exporters	Internal Hosts
Up to 10,000	2	24 GB	200 GB	Up to 65535	Up to 1024	25,000
Up to 30,000	6	32 GB	200 GB	Up to 65535	Up to 1024	50,000
Up to 60,000	8	64 GB	200 GB	Up to 65535	Up to 2048	100,000
Up to 120,000	12	128 GB	200 GB	Up to 65535	Up to 4096	250,000

Data Node Virtual Edition

Review the following information to calculate resource requirements for the Data Node Virtual Edition.

- **Calculate Flows Per Second:** Determine the flows per second expected on the network. Refer to the [Calculating Flows Per Second](#) section for details.
- **Number of Data Nodes:** You can deploy 1 Data Node or 3 or more Data Nodes (in sets of 3). For details, refer to [Appliance Requirements \(with Data Store\)](#).

Based on your [Flows Per Second](#) calculations, refer to the following specifications to determine your resource requirements:

Data Store with a Single Virtual Data Node

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage for Single Data Node for 30 Days of Retention
Up to 30,000	6	32 GB	2.25 TB
Up to 60,000	6	32 GB	4.5 TB
Up to 120,000	12	32 GB	9 TB
Up to 225,000	18	64 GB	18 TB

Data Store with 3 Virtual Data Nodes

Flows per second	Required Reserved CPUs	Required Reserved Memory	Required Minimum Storage for each Data Node for 30 Days of Retention	Required Minimum Storage for 3 Data Node Data Store for 30 Days of Retention
Up to 30,000	6	32 GB	1.5 TB per Data Node	4.5 TB total for Data Store
Up to 60,000	6	32 GB	3 TB per Data Node	9 TB total for Data Store
Up to 120,000	12	32 GB	6 TB per Data Node	18 TB total for Data Store
Up to 220,000	18	64 GB	10 TB per Data Node*	30 TB total for Data Store*
Up to 500,000	18	64 GB	15 TB per Data Node*	45 TB total for Data Store*
* At scale Data Store optimizations are applied to reduce linear growth of telemetry				

Flow Sensor Virtual Edition

This section describes the Flow Sensor Virtual Edition.

- **Cache:** The Flow Cache Size column indicates the maximum number of active flows that the Flow Sensor can process at the same time. The cache adjusts with the amount of reserved memory, and flows are flushed every 60 seconds. Use the Flow Cache Size to calculate the amount of memory needed for the amount of traffic being monitored.
- **Requirements:** Your environment may require more resources depending on a number of variables, such as average packet size, burst rate, and other network and host conditions.

NICs - monitoring ports	Required Reserved CPUs	Required Minimum Reserved Memory	Required Minimum Data Storage	Estimated Throughput	Flow Cache Size (maximum number of concurrent flows)
1 x 1 Gbps	2	4 GB	75 GB	850 Mbps	32,766
2 x 1 Gbps	4	8 GB	75 GB	1,850 Mbps Interfaces configured as PCI pass-through (igb/ixgbe compliant or e1000e compliant)	65,537
4 x 1 Gbps	8	16 GB	75 GB	3,700 Mbps Interfaces configured as PCI pass-through	131,073

NICs - monitoring ports	Required Reserved CPUs	Required Minimum Reserved Memory	Required Minimum Data Storage	Estimated Throughput	Flow Cache Size (maximum number of concurrent flows)
				(igb/ixgbe compliant or e1000e compliant)	
1 x 10 Gbps*	12	24 GB	75 GB	8 Gbps Interfaces configured as PCI pass-through (Intel ixgbe/i40e compliant)	~512,000
2 x 10 Gbps*	22	40 GB	75 GB	16 Gbps Interfaces configured as PCI pass-through (Intel ixgbe/i40e compliant)	~1,000,000

*For 10 Gbps throughput, configure all CPUs in 1 socket. For each additional 10 Gbps NIC, add 10 vCPUs and 16 GB of RAM.

Optional: One or more 10G NICs may be used on the physical VM host.

Flow Sensor Virtual Edition Network Environments

Before installing the Flow Sensor Virtual Edition, make sure you know the type of network environment you have. This guide covers all types of network environments that a Flow Sensor Virtual Edition can monitor.

Compatibility: Secure Network Analytics supports a VDS environment, but it does not support VMware Distributed Resource Scheduler (VM-DRS).

Virtual Network Environments: The Flow Sensor Virtual Edition monitors the following types of virtual network environments:

- A network with virtual local area network (VLAN) trunking
- Discrete VLANs where one or more VLANs are prohibited from attaching packet monitoring devices (for example, due to local policy)
- Private VLANs
- Hypervisor hosts rather than VLANs

Flow Sensor Virtual Edition Traffic

The Flow Sensor will process traffic with the following Ethertypes:

Ethertype	Protocol
0x8000	Normal IPv4
0x86dd	Normal IPv6
0x8909	SXP
0x8100	VLAN
0x88a8 0x9100 0x9200 0x9300	VLAN QnQ
0x8847	MLPS unicast
0x8848	MLPS multicast



The Flow Sensor saves the top-level MPLS label or VLAN ID and exports it. It bypasses the other labels when it is processing packets.

UDP Director Virtual Edition

The UDP Director Virtual Edition requires that the virtual machine meets the following specifications. Also, the minimum storage space may increase based on your FPS calculation and your retention requirements.

Required Reserved CPU	Required Reserved Memory	Minimum Data Storage	Maximum FPS Rate
2	4 GB	75 GB	10,000

Calculating Flows Per Second (Optional)

If you want to calculate your resource requirements based on a different storage amount than we have provided in the previous sections, you can use the Flows per Second (FPS) calculations shown here.

Calculating Flows Per Second for Flow Collector Storage (Deployments without Data Store)

If you deploy a Flow Collector (NetFlow) without a Data Store, calculate the storage allocation as follows:

$[(\text{daily average FPS}/1,000) \times 1.6 \times \text{days}]$

- Determine your daily average FPS
- Divide this number by 1,000 FPS
- Multiply this number by 1.6 GB of storage for one day's worth of storage
- Multiply this number by the number of days you want to store the flows for total storage on the Flow Collector

For example, if your system:

- has 50,000 daily average FPS
- will store flows for 30 days,

calculate per Flow Collector as follows:

$[(50,000/1,000) \times 1.6 \times 30] = 7200 \text{ GB (7.2 TB)}$

- daily average FPS = 50,000
- $50,000 \text{ daily average FPS} / 1,000 = 50$
- $50 \times 1.6 \text{ GB} = 80 \text{ GB}$ for one day's worth of storage
- $80 \text{ GB} \times 30 \text{ days per Flow Collector} = 7200 \text{ GB per Flow Collector}$

Calculating Flows Per Second for Data Node Storage

If you deploy a Data Store Virtual Edition with 3 Data Nodes Virtual Edition, we recommend that for each Data Node, calculate the storage allocation as follows:

$[(\text{daily average FPS}/1,000) \times 1.6 \times \text{days}] / \text{number of Data Nodes}$

- Determine your daily average FPS
- Divide this number by 1,000 FPS
- Multiply this number by 1.6 GB of storage for one day's worth of storage

- Multiply this number by the number of days you want to store the flows for total Data Store storage
- Divide this number by the number of Data Nodes in your Data Store for storage per Data Node

For example, if your system:

- has 50,000 daily average FPS
- will store flows for 90 days, and
- you have 3 Data Nodes

calculate per Data Node as follows:

$$[(50,000/1,000) \times 1.6 \times 90] / 3 = 2400 \text{ GB (2.4 TB) per Data Node}$$

- daily average FPS = 50,000
- $50,000 \text{ daily average FPS} / 1,000 = 50$
- $50 \times 1.6 \text{ GB} = 80 \text{ GB}$ for one day's worth of storage
- $80 \text{ GB} \times 90 \text{ days per Data Store} = 7200 \text{ GB per Data Store}$
- $7200 \text{ GB} / 3 \text{ Data Nodes} = 2400 \text{ GB (2.4 TB) per Data Node}$

1. Configuring Your Firewall for Communications

In order for the appliances to communicate properly, you should configure the network so that firewalls or access control lists do not block the required connections. Use the information provided in this section to configure your network so that the appliances can communicate through the network.

Open Ports (All Appliances)

Consult with your network administrator to ensure that the following ports are open and have unrestricted access on your appliances (Managers, Flow Collectors, Data Nodes, Flow Sensors, and UDP Directors):

- 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

Additional Open Ports for Data Nodes

In addition, if you deploy Data Nodes to your network, ensure that the following ports are open and have unrestricted access:

- TCP 5433
- TCP 5444
- TCP 9450

Communication Ports and Protocols

The following table shows how the ports are used in Secure Network Analytics:

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
Active Directory	Manager	TCP/389, UDP/389	LDAP
Cisco ISE	Manager	TCP/443	HTTPS
Cisco ISE	Manager	TCP/8910	XMPP
External log sources	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	3rd Party event management systems	UDP/514	SYSLOG
Flow Sensor	Manager	TCP/443	HTTPS
Flow Sensor	Flow Collector (NetFlow)	UDP/2055	NetFlow
NetFlow Exporters	Flow Collector (NetFlow)	UDP/2055*	NetFlow
sFlow Exporters	Flow Collector (sFlow)	UDP/6343*	sFlow
Manager	UDP Director	TCP/443	HTTPS
Manager	Cisco ISE	TCP/443	HTTPS

From (Client)	To (Server)	Port	Protocol
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 Exporters	UDP/161	SNMP
Manager	LDAP	TCP/636	TLS
Manager	CRL Distribution Points	TCP/80	HTTP
Manager	OCSP responders	TCP/80	OCSP
User PC	Manager	TCP/443	HTTPS

*This is the default port, but any UDP port could be configured on the exporter.

Additional Open Ports for Data Store

The following lists the communication ports to open on your firewall to deploy the Data Store.

#	From (Client)	To (Server)	Port	Protocol or Purpose
1	Manager	Flow Collectors and Data Nodes	22/TCP	SSH, required to initialize Data Store database
1	Data Nodes	all other Data Nodes	22/TCP	SSH, required to initialize Data Store database and for database administration tasks
2	Manager, Flow Collectors, and Data Nodes	NTP server	123/UDP	NTP, required for time synchronization
2	NTP server	Manager, Flow Collectors, and Data Nodes	123/UDP	NTP, required for time synchronization
3	Manager	Flow Collectors and Data Nodes	443/TCP	HTTPS, required for secure communications between appliances
3	Flow Collectors	Manager	443/TCP	HTTPS, required for secure communications between appliances
3	Data Nodes	Manager	443/TCP	HTTPS, required for secure communications between appliances
4	NetFlow Exporters	Flow Collectors - NetFlow	2055/UDP	NetFlow ingestion
5	Data Nodes	all other Data Nodes	4803/TCP	inter-Data Node messaging service
6	Data Node	all other Data	4803/UDP	inter-Data Node messaging

		Nodes		service
7	Data Nodes	all other Data Nodes	4804/UDP	inter-Data Node messaging service
8	Manager, Flow Collectors, and Data Nodes	Data Nodes	5433/TCP	Vertica client connections
9	Data Node	all other Data Node	5433/UDP	Vertica messaging service monitoring
10	sFlow Exporters	Flow Collector (sFlow)	6343/UDP	sFlow ingestion
11	Data Nodes	all other Data Nodes	6543/UDP	inter-Data Node messaging service

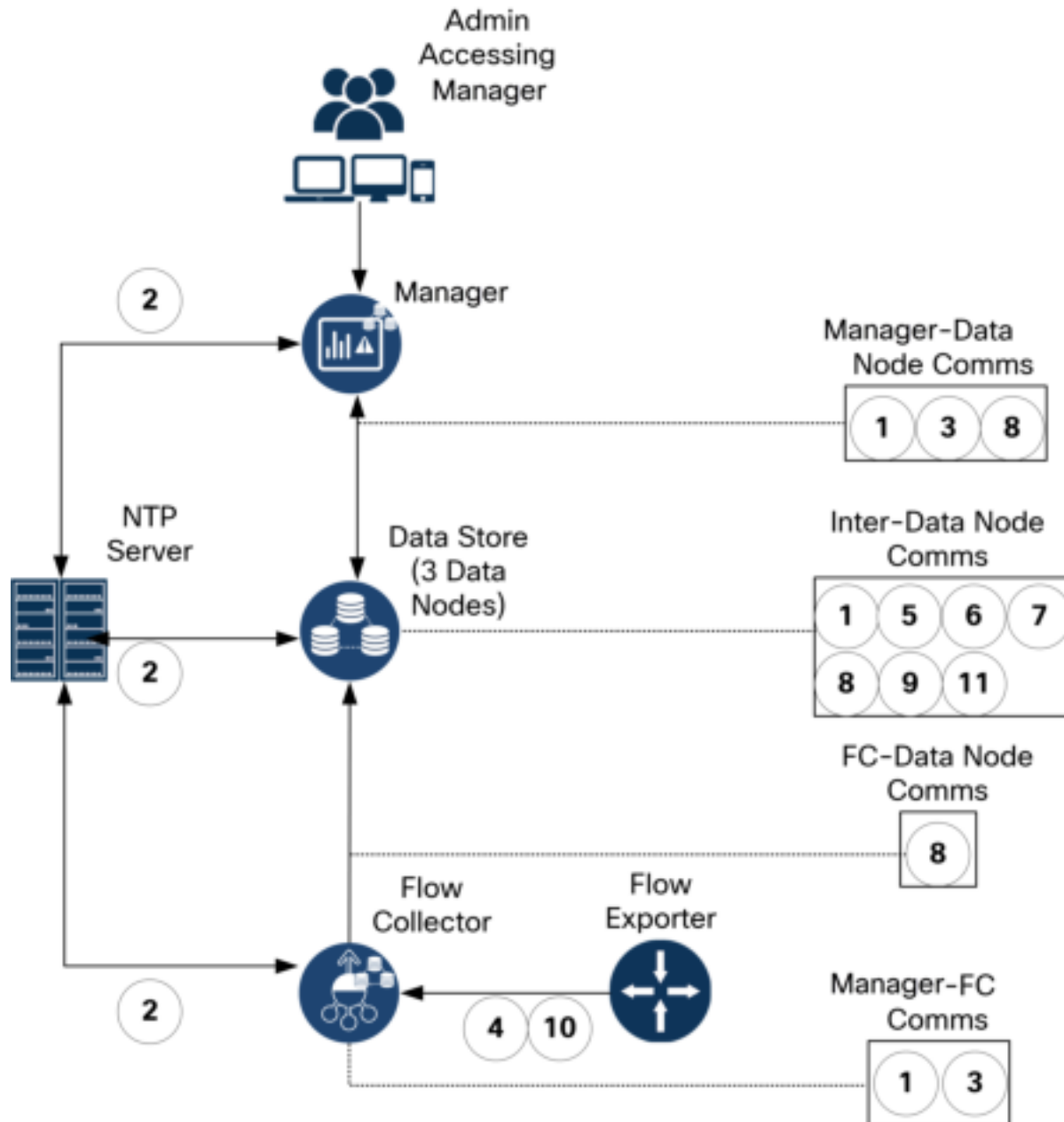
Optional Communication Ports

The following table is for optional configurations determined by your network needs:

From (Client)	To (Server)	Port	Protocol
All appliances	User PC	TCP/22	SSH
Manager	3rd Party event management systems	UDP/162	SNMP-trap
Manager	3rd Party event management systems	UDP/514	SYSLOG
Manager	Email gateway	TCP/25	SMTP
Manager	Threat Feed	TCP/443	SSL
User PC	All appliances	TCP/22	SSH

Secure Network Analytics Deployment with Data Store Example

As shown in the figure below, you can strategically deploy Secure Network Analytics appliances to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



2. Downloading Virtual Edition Installation Files

Use the following instructions to download the ISO files for your virtual appliance installation.

Installation Files

Virtual Machine	Appliance Installation File	Details
3a. VMware vCenter	ISO	Installing your virtual appliances using VMware vCenter.
3b. VMware ESXi Stand-Alone Server	ISO	Installing your virtual appliances on an ESXi stand-alone host server.
3c. KVM and Virtual Machine Manager	ISO	Installing your virtual appliances using KVM and Virtual Machine Manager.

1. Log in to Cisco Software Central

1. Log in to Cisco Software Central at <https://software.cisco.com>.
2. In the **Download and manage** > **Download and Upgrade** section, select **Access downloads**.
3. Scroll down until you see the **Select a Product** field.
4. You can access Secure Network Analytics files in two ways:
 - **Search by Name:** Type **Secure Network Analytics** in the **Select a Product** field. Press Enter.
 - **Search by Menu:** Click Browse All. Select **Security** > **Network Visibility and Segmentation** > **Secure Analytics (Stealthwatch)**.

2. Download Files

1. Select an appliance type.
 - Secure Network Analytics Virtual Manager
 - Secure Network Analytics Virtual Flow Collector
 - Secure Network Analytics Virtual Flow Sensor
 - Secure Network Analytics Virtual UDP Director
 - Secure Network Analytics Virtual Data Store
2. Select **Secure Network Analytics System Software**.
3. In the Latest Release column, select **7.4.2** (or the version of 7.4.x that you are installing).
4. **Download:** Locate the ISO installation file. Click the **Download** icon or **Add to Cart** icon.
5. Repeat these instructions to download the files for each appliance type.

3a. Installing a Virtual Appliance using VMware vCenter (ISO)

Overview

Use the following instructions to install your virtual appliances using **VMware vCenter**. To use an alternative method, refer to the following:

- **VMware ESXi Stand-Alone Server:** Use [3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server \(ISO\)](#).
- **KVM:** Use [3c. Installing a Virtual Appliance on a KVM Host \(ISO\)](#).



Secure Network Analytics v7.4.2 is compatible with VMware 7.0 or 8.0. We do not support VMware 6.0, 6.5, or 6.7 with Secure Network Analytics v7.4.x. For more information, refer to VMware documentation for vSphere 6.0, 6.5, and 6.7 End of General Support.

Before You Begin

Before you begin the installation, complete the following preparation procedures:

1. **Compatibility:** Review the compatibility requirements in [Compatibility](#).
2. **Resource Requirements:** Review the [Resource Requirements](#) section to determine the required allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
3. **Firewall:** Configure your firewall for communications. Refer to [1. Configuring Your Firewall for Communications](#).
4. **Files:** Download the appliance ISO files. Refer to [2. Downloading Virtual Edition Installation Files](#) for instructions.
5. **Time:** Confirm the time set on the hypervisor host in your VMware environment (where you will be installing the virtual appliance) shows the correct time. Otherwise, the virtual appliances may not be able to boot up.



Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Secure Network Analytics appliances.



Do not install VMware Tools on a Secure Network Analytics virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

Installing a Virtual Appliance Using vCenter (ISO)

If you have VMware vCenter (or similar), use the following instructions to install a virtual appliance using the ISO.

If you are deploying Data Nodes or Flow Sensors, make sure you complete all required procedures.

Data Nodes

Complete the following procedures:

1. Configuring an Isolated LAN for inter-Data Node Communications.

3. Installing the Virtual Appliance. When you install the Data Node virtual appliance, you also need to install [two network adapters](#).

Flow Sensors

Complete the following procedures:

2. Configuring the Flow Sensor to Monitor Traffic

3. Installing the Virtual Appliance

4. Defining Additional Monitoring Ports (Flow Sensors only)

All Other Appliances

If the appliance is not a Data Node or Flow Sensor, complete the following procedure:

3. Installing the Virtual Appliance



Some of the menus and graphics may vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. Configuring an Isolated LAN for inter-Data Node Communications

If you are deploying Data Nodes Virtual Edition to your network, configure an isolated LAN with a virtual switch so that the Data Nodes can communicate with each other over **eth1** for inter-Data Node communication.

There are two options for configuring switches:

- **Configuring a vSphere Standard Switch**
- **Configuring a vSphere Distributed Switch**

Configuring a vSphere Standard Switch

1. Log into your VMware host environment.
2. Follow the [VMware Create a vSphere Standard Switch documentation](#) for configuring a vSphere Standard Switch. Note that in step 4, you will want to choose the Virtual Machine Port Group for a Standard Switch option.
3. Go to **3. Installing the Virtual Appliance**.

Configuring a vSphere Distributed Switch

1. Log into your VMware host environment.
2. Follow the [VMware Create a vSphere Distributed Switch](#) documentation for configuring a vSphere Distributed Switch. Note that for the number of uplinks in step 5a, there is a requirement of at least 1 uplink, however it is not necessary to configure an uplink unless you are distributing the nodes across multiple hosts. If you need to distribute nodes across multiple hosts, contact [Cisco Support](#) for assistance.
3. Go to **3. Installing the Virtual Appliance**.

2. Configuring the Flow Sensor to Monitor Traffic

The Flow Sensor Virtual Edition has the ability to provide visibility into VMware environments, generating flow data for areas that are not flow-enabled. As a virtual appliance installed inside each hypervisor host, the Flow Sensor Virtual Edition passively captures Ethernet frames from the host vSwitch, and it observes and creates flow records containing valuable session statistics that pertain to conversational pairs, bit rates, and packet rates.



You will need to install a Flow Sensor on each host within the environment you want to monitor.

Use the following instructions to configure the Flow Sensor Virtual Edition to monitor traffic on a vSwitch as follows:

- [Monitoring a vSwitch with Multiple Hosts](#)
- [Monitoring a vSwitch with a Single Host](#)

Monitoring External Traffic with PCI Pass-Through

You can also configure your Flow Sensor Virtual Edition for direct network monitoring using a compliant PCI pass-through.

- **Requirements:** igb/ixgbe compliant or e1000e compliant PCI pass-through.
- **Resource Information:** Refer to [Flow Sensor Virtual Edition](#).
- **Integration:** Refer to [1. Configuring Your Firewall for Communications](#).
- **Instructions:** To add PCI network interfaces to the Flow Sensor Virtual Edition, refer to your VMware documentation.

Monitoring a vSwitch with Multiple Hosts

Use the instructions in this section to use the Flow Sensor Virtual Edition to monitor traffic on a Distributed vSwitch that spans multiple VM hosts or clusters.

This section applies only to VDS networks. If your network is in a non-VDS environment, go to [Monitoring a vSwitch with a Single Host](#).

Configuration Requirements



You will need to install a Flow Sensor on each host within the environment you want to monitor.

This configuration has the following requirements:

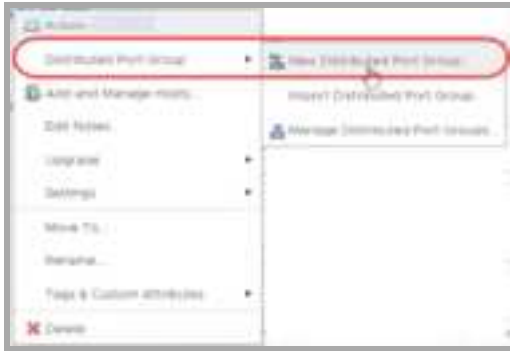
- **Distributed Virtual Port (dvPort):** Add a dvPort group with the correct VLAN settings for each VDS that the Flow Sensor Virtual Edition will monitor. If the Flow Sensor Virtual Edition monitors both VLAN and non-VLAN traffic on the network, you need to create two dvPort groups, one for each type.
- **VLAN Identifier:** If your environment uses a VLAN (other than VLAN trunking or a private VLAN), you need the VLAN identifier to complete this procedure.
- **Promiscuous Mode:** Enabled.
- **Promiscuous Port:** Configured to the vSwitch.

Complete the following steps to configure the network using a VDS:

1. Click the **Networking** icon.



2. In the Networking tree, right-click the VDS.
3. Select **Distributed Port Group** > **New Distributed Port Group**.



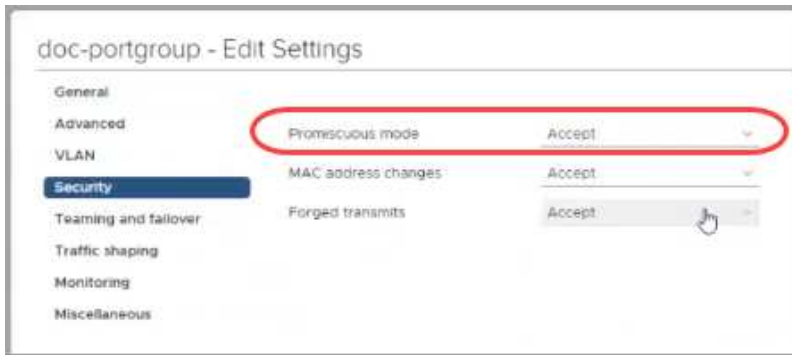
4. Use the **New Distributed Port Group** dialog box to configure the port group, including the specifications in the following steps.
5. **Select Name and Location:** In the **Name** field, enter a name to identify this dvPort group.
6. **Configure Settings:** In the **Number of Ports** field, enter the number of Flow Sensor Virtual Editions in your cluster of hosts.

7. Click the **VLAN type** drop-down list.
 - If your environment doesn't use a VLAN, select **None**.
 - If your environment uses a VLAN, select the VLAN type. Configure it as follows:

VLAN Type	Detail
VLAN	In the VLAN ID field, enter the number

	(between 1 and 4094) that matches the identifier.
VLAN Trunking	In the VLAN trunk range field, enter 0-4094 to monitor all VLAN traffic.
Private VLAN	Select Promiscuous from the drop-down list.

8. **Ready to Complete:** Review the configuration settings. Click **Finish**.
9. In the Networking tree, right-click the new dvPort group. Select **Edit Settings**.
10. Select **Security**.
11. Click the **Promiscuous Mode** drop-down list. Select **Accept**.



12. Click **OK** to close the dialog box.
13. Does the Flow Sensor Virtual Edition monitor both VLAN and non-VLAN network traffic?
 - If yes, repeat the steps in this section [Monitoring a vSwitch with Multiple Hosts](#).
 - If no, continue to the next step.
14. Is there another VDS in the VMware environment that the Flow Sensor Virtual Edition will monitor?
 - If yes, repeat the steps in this section [Monitoring a vSwitch with Multiple Hosts](#) for the next VDS.
15. Go to [3. Installing the Virtual Appliance](#).

Monitoring a vSwitch with a Single Host

Use the instructions in this section to use the Flow Sensor Virtual Edition to monitor traffic on a vSwitch with a single host.



This section applies only to non-VDS networks. If your network uses a VDS, go to [Monitoring a vSwitch with Multiple Hosts](#).

Configuration Requirements

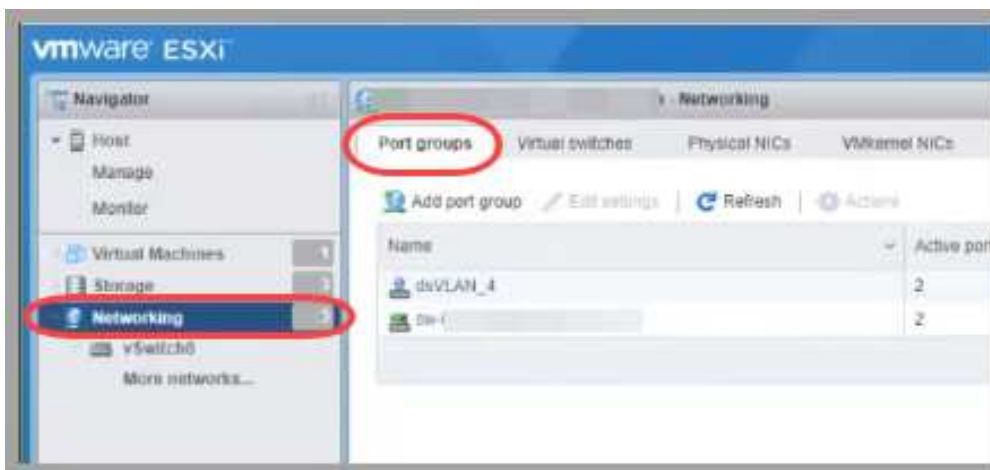
This configuration has the following requirements:

- **Promiscuous Port Group:** Add a promiscuous port group for each virtual switch that the Flow Sensor Virtual Edition will be monitoring.
- **Promiscuous Mode:** Enabled.
- **Promiscuous Port:** Configured to the vSwitch.

Configure the Port Group to Promiscuous Mode

Use the following instructions to add a port group, or edit a port group, and set it to Promiscuous.

1. Log in to your VMware ESXi host environment.
2. Click **Networking**.



3. Select the **Port groups** tab.
4. You can create a new port group or edit a port group.

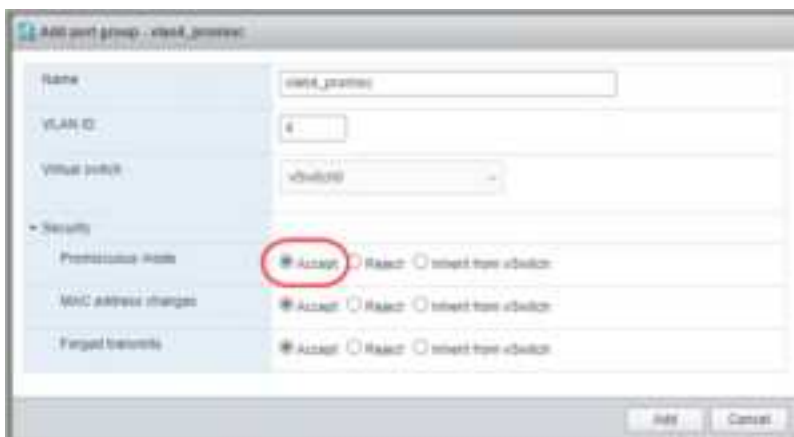
- **Create Port Group:** Click **Add port group**.
 - **Edit Port Group:** Select the port group. Click **Edit Settings**.
5. Use the dialog box to configure the port group. Configure the VLAN ID or VLAN Trunking:

VLAN Type	Detail
VLAN ID	Use VLAN ID to specify a single VLAN. In the VLAN ID field, enter the number (between 1 and 4094) that matches the identifier.
VLAN Trunking	Use VLAN Trunking to monitor all VLAN traffic. The range defaults to 0-4095.

6. Click the **Security** arrow.



7. **Promiscuous Mode:** Choose **Accept**.



8. Will the Flow Sensor Virtual Edition be monitoring another virtual switch in this VMware environment?

If yes, go back to **2. Configuring the Flow Sensor to Monitor Traffic**, and repeat all the steps for the next virtual switch.

9. Go to **3. Installing the Virtual Appliance**

3. Installing the Virtual Appliance

Use the following instructions to install a virtual appliance on your hypervisor host and define the virtual appliance management and monitoring ports.



Some of the menus and graphics may vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. Log in to your VMware Web Client.
2. Locate the virtual appliance software file (ISO) that you downloaded from [Cisco Software Central](#).
3. Make the ISO available in vCenter. You have the following options:
 - Upload the ISO to a vCenter datastore.
 - Add the ISO to a content library.
 - Keep the ISO on your local workstation, and configure the deployment to reference that file.

See the VMware documentation for more information.

4. From the vCenter UI, select **Menu > Hosts and Clusters**.
5. In the navigation pane, right click a cluster or host and select **New Virtual Machine...** to access the New Virtual Machine wizard.
6. From the Select a creation type window, select **Create a new virtual machine**, then click **Next**.



7. From the Select a name and folder window, enter a **Virtual machine name**, select a **location for the virtual machine**, then click **Next**.



8. From the Select a compute resource window, select a cluster, host, resource pool, or vApp to which you will deploy the appliance, then click **Next**.



9. From the Select storage window, select a **VM Storage Policy** from the drop-down, then select a storage location, then click **Next**.



10. From the Select compatibility window, select a virtual machine version from the **Compatible with** drop-down, based on your current deployed ESXi version. For example, the following screenshot shows **ESXi 7.0 and later** because ESXi 7.0 is deployed. Click **Next**.



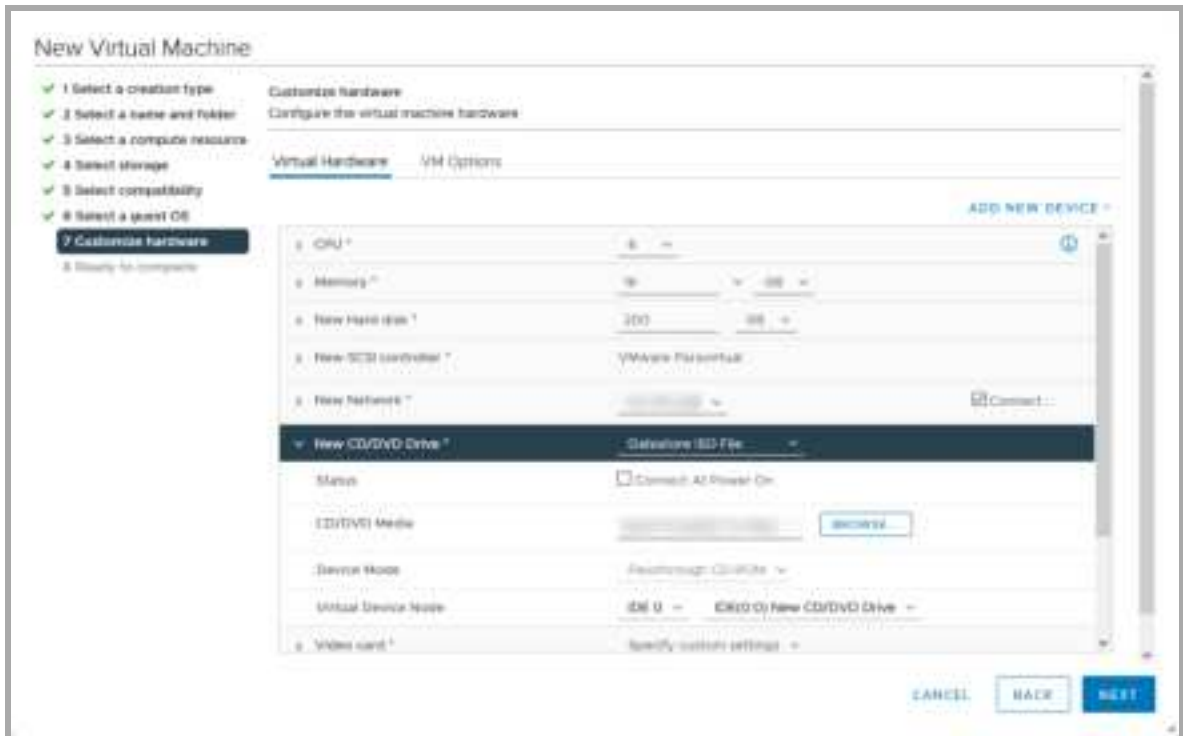
11. From the Select a guest OS screen, select the **Linux Guest OS Family** and the **Debian GNU/Linux 11 (64-bit) Guest OS Version**. Click **Next**.



12. From the Customize hardware window, configure the virtual hardware. Refer to [Resource Requirements](#) for specific recommendations for your appliance type.



This step is critical for system performance. If you choose to deploy Cisco Secure Network Analytics appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.



In addition to the resource requirements, make sure the following settings are selected:

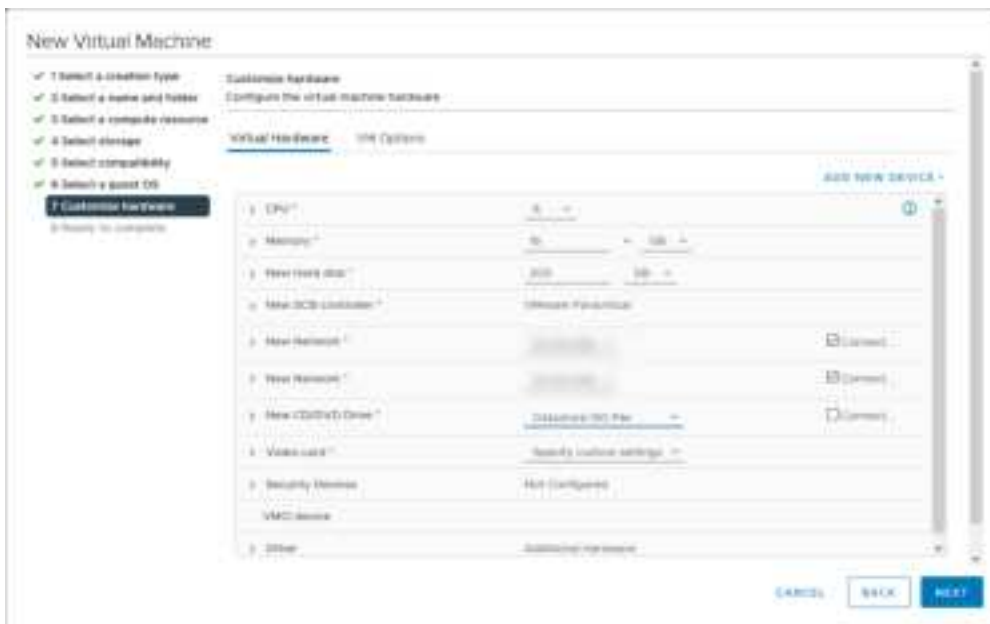
- Click **New Hard disk** to expand the configuration options. Select **Thick Provision Lazy Zeroed** from the **Disk Provisioning** drop-down.
 - Click **New SCSI controller** to expand the configuration options. Select **LSI Logic SAS** from the **Change Type** drop-down. If you do not select **LSI Logic SAS**, your virtual appliance may fail to properly deploy.
 - In the **New CD/DVD Drive** field, select an ISO location based on where you have stored the ISO. Click **New CD/DVD Drive** to expand the configuration options. Check **Connect At Power On**.
 - **If the appliance is a Flow Sensor**, and you are configuring 10 Gbps throughput for the NIC, click **CPU** to expand the configuration options. Configure all **Cores per Socket** so all CPUs are in one socket.
13. **Data Nodes:** If you are deploying a Data Node virtual appliance, also add a second network adaptor.

Click **Add New Device**, then select **Network Adapter** and ensure the Adapter Type is **VMXNET3**.

- For the **first network adaptor**, select a switch that will allow the Data Node Virtual Edition to communicate on a public network with other appliances.
- For the **second network adaptor**, select the switch that you created in **1. Configuring an Isolated LAN for inter-Data Node Communications** that will allow the Data Node Virtual Edition to communicate on a private network with other Data Nodes.



Ensure that you properly assign the network adaptors and virtual switches for every Data Node in your deployment as you deploy each Data Node.



14. From the Ready to complete window, review your settings, then click **Finish**.



15. The deployment starts when you click the **Power On** icon. Monitor the deployment progress in the **Recent Tasks** section. Make sure the deployment is completed and shown in the Inventory tree before you go to the next steps.
16. Next Steps:
- **Flow Sensors:** If the appliance is a Flow Sensor and will be monitoring more than one virtual switch in the VMware environment, or more than one VDS in a cluster, continue with the next section [4. Defining Additional Monitoring Ports \(Flow Sensors only\)](#).
 - **All Other Appliances:** Repeat all of the procedures in this section [3. Installing the Virtual Appliance](#) to deploy another virtual appliance.
17. If you have finished installing all virtual appliances in your system, go to [4. Configuring Your Secure Network Analytics System](#).

4. Defining Additional Monitoring Ports (Flow Sensors only)

This procedure is required if the Flow Sensor Virtual Edition will be monitoring more than one virtual switch in a VMware environment or more than one VDS in a cluster.



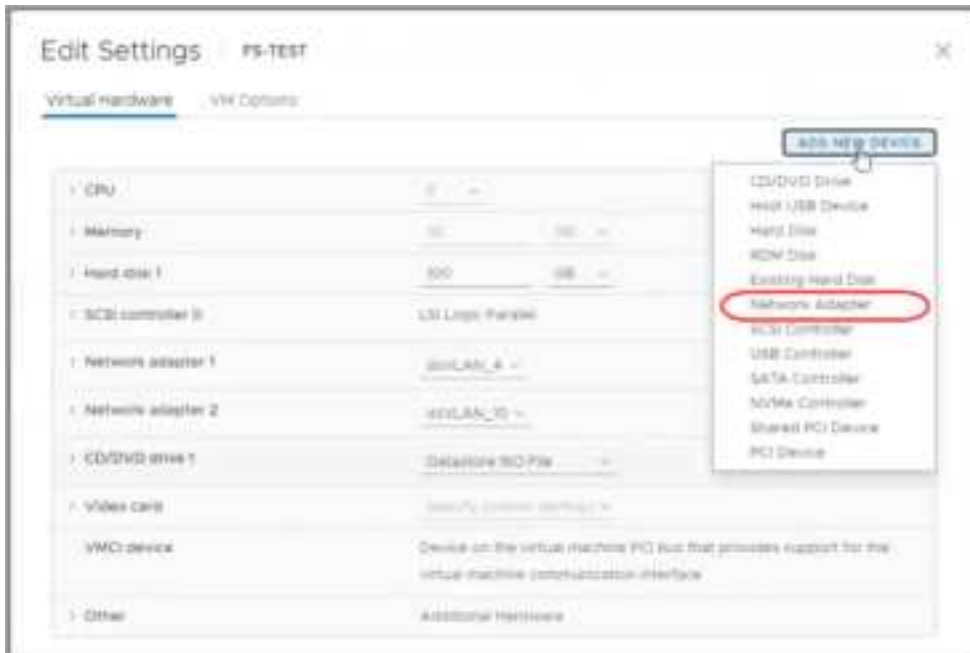
If this is not the monitoring configuration for your Flow Sensor, you do not need to complete this procedure.

To add Flow Sensor Virtual Edition monitoring ports, complete the following steps:

1. In the Inventory tree, right-click the Flow Sensor Virtual Edition. Select **Edit Settings**.

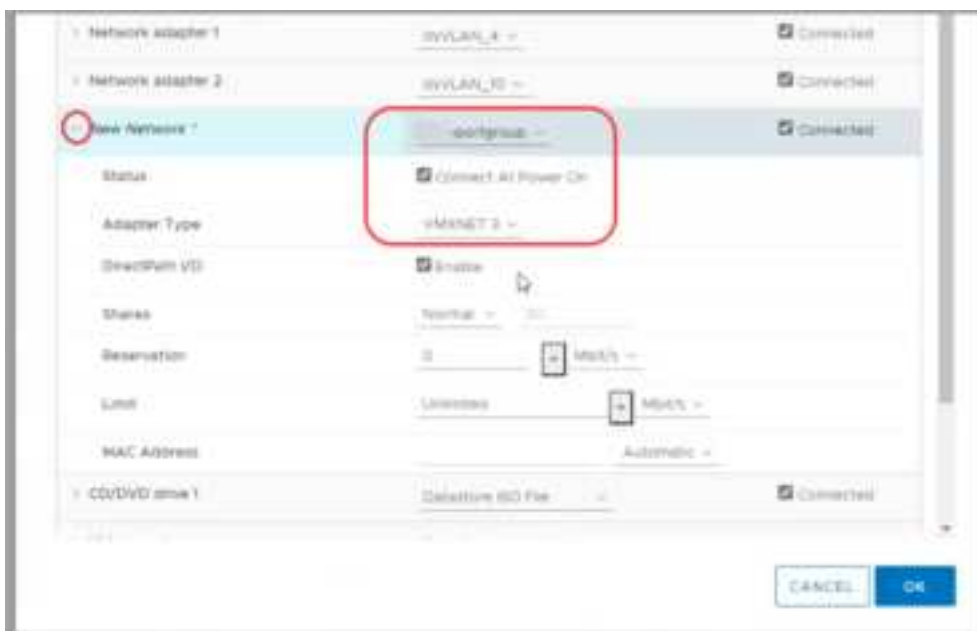


2. Use the **Edit Settings** dialog box to configure the following specified settings.
3. Click **Add New Device**. Select **Network Adapter**.



4. Locate the new network adapter. Click the arrow to expand the menu, and configure the following:

- **New Network:** Select an unassigned promiscuous port group.
- **Adapter Type:** Select **VMXNET 3**.
- **Status:** Check the **Connect at Power On** check box.



5. After reviewing the settings, click **OK**.
6. Repeat this procedure to add another Ethernet adapter as needed.
7. Next Steps:
 - **Flow Sensors:** To configure another Flow Sensor, go to [2. Configuring the Flow Sensor to Monitor Traffic](#).
 - **All Other Appliances:** Repeat all of the procedures in this section [3. Installing the Virtual Appliance](#) to deploy another virtual appliance.
 - If you have completed installing all virtual appliances in your system, go to [4. Configuring Your Secure Network Analytics System](#).

3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)

Overview

Use the following instructions to install your virtual appliances using a **VMware environment with an ESXi Stand-alone server**.



Secure Network Analytics v7.4.2 is compatible with VMware v7.0 or 8.0. We do not support VMware v6.0, v6.5, or v6.7 with Secure Network Analytics v7.4.x. For more information, refer to VMware documentation for vSphere 6.0, 6.5, and 6.7 End of General Support.

To use an alternative method, refer to the following:

- **VMware vCenter:** Use [3a. Installing a Virtual Appliance using VMware vCenter \(ISO\)](#).
- **KVM:** Use [3c. Installing a Virtual Appliance on a KVM Host \(ISO\)](#).

Before You Begin

Before you begin the installation, complete the following preparation procedures:

1. **Compatibility:** Review the compatibility requirements in [Compatibility](#).
2. **Resource Requirements:** Review the [Resource Requirements](#) section to determine the required allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
3. **Firewall:** Configure your firewall for communications. Refer to [1. Configuring Your Firewall for Communications](#).
4. **Files:** Download the appliance ISO files. Refer to [2. Downloading Virtual Edition Installation Files](#) for instructions.
5. **Time:** Confirm the time set on the hypervisor host in your VMware environment (where you will be installing the virtual appliance) shows the correct time. Otherwise, the virtual appliances may not be able to boot up.



Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Secure Network Analytics appliances.



Do not install VMware Tools on a Secure Network Analytics virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

Installing a Virtual Appliance on an ESXi Stand-Alone Server (ISO)

Use the following instructions to install your virtual appliances using a **VMware environment with an ESXi Stand-alone server**.

Process Overview

Installing a virtual appliance involves completing the following procedures, which are covered in this chapter:

1. **Logging in to the VMware Web Client**
2. **Booting from the ISO**

Data Nodes

If you are deploying Data Nodes, follow the instructions in the previous section **1. Configuring an Isolated LAN for inter-Data Node Communications** before you complete the procedures in this section.

1. Logging in to the VMware Web Client



Some of the menus and graphics may vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. Log in to the VMware Web Client.
2. Click **Create/Register a Virtual Machine**.
3. Use the **New Virtual Machine** dialog box to configure the appliance as specified in the following steps.
4. **Select Creation Type:** Select **Create a New Virtual Machine**.



5. **Select a Name and Guest OS:** Enter or select the following:

- **Name:** Enter a name for the appliance so you can identify it easily.
- **Compatibility:** Select the version you are using (v7.0 or 8.0).
- **Guest OS family:** Linux.
- **Guest OS version:** Select **Debian GNU/Linux 11 64-bit**.



6. **Select Storage:** Select an accessible datastore. Review [Resource Requirements](#) to confirm you have enough space.



Review [Resource Requirements](#) to allocate sufficient resources. This step is critical for system performance.

 If you choose to deploy Cisco Secure Network Analytics appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

7. **Customize Settings:** Enter or select your appliance requirements (refer to [Resource Requirements](#) for details).

Make sure you select the following:

- **SCSI Controller:** LSI Logic SAS
- **Network Adapter:** Confirm the management address for the appliance.
- **Hard Disk:** Thick Provisioning Lazy Zeroed

If the appliance is a Flow Sensor, you can click **Add Network Adapter** to add another management or sensing interface.

If the appliance is a Flow Sensor, and you are configuring 10 Gbps throughput for the NIC, click **CPU** to expand the configuration options. Configure all all CPUs in one socket.

If the appliance is a Data Node, add another network interface to allow inter-Data Node communications. Click **Add Network Adapter**.

- For the **first network adaptor**, select a switch that will allow the Data Node Virtual Edition to communicate on a public network with other appliances.
- For the **second network adaptor**, select the switch that you created in [1. Configuring an Isolated LAN for inter-Data Node Communications](#) that will allow the Data Node Virtual Edition to communicate on a private network with other Data Nodes.



8. Click the arrow next to Network Adapter.
9. For the Adapter Type, select **VMXnet3**.

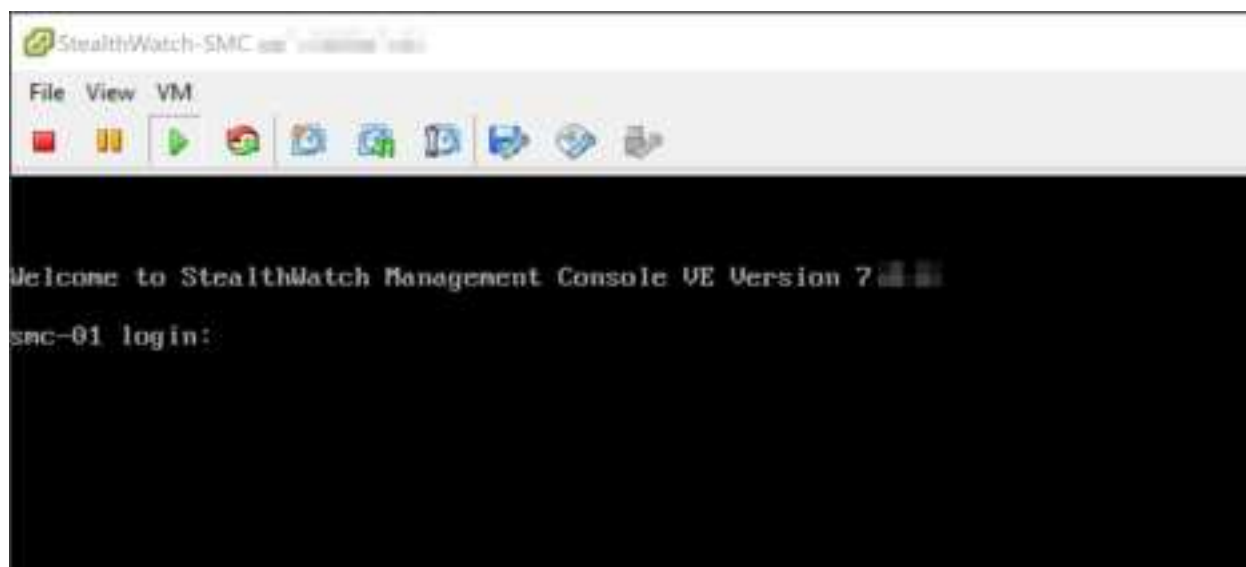


While Cisco supports the use of E1000 (1G dvSwitch), 1G PCI-passthrough, and VMXNET 3 interfaces, Cisco strongly recommends that you use the VMXNET3 interface as it has been proven to provide the best network performance for Cisco virtual appliances.

10. Review your configuration settings and confirm they are correct.
11. Click **Finish**. A virtual machine container is created.

2. Booting from the ISO

1. Open the VMware console.
2. Connect the ISO to the new virtual machine. Refer to the VMware guide for details.
3. Boot the virtual machine from the ISO. It runs the installer and reboots automatically.
4. Once the installation and reboot are completed, you will see the login prompt.



5. Disconnect the ISO from the virtual machine.
6. Repeat all of the procedures in [3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server \(ISO\)](#) for the next virtual appliance.
7. **Flow Sensors:** If the appliance is a Flow Sensor, finish the setup using the previous sections of this manual:
 - [2. Configuring the Flow Sensor to Monitor Traffic](#) (use Monitoring a vSwitch with a Single Host)
 - If the Flow Sensor will be monitoring more than one virtual switch in the VMware environment, or more than one VDS in a cluster, go to [4. Defining Additional Monitoring Ports \(Flow Sensors only\)](#).
8. If you have completed installing all virtual appliances in your system, go to [4. Configuring Your Secure Network Analytics System](#).

3c. Installing a Virtual Appliance on a KVM Host (ISO)

Overview

Use the following instructions to install your virtual appliances using **KVM and Virtual Machine Manager**.

To use an alternative method, refer to the following:

- **VMware vCenter:** Use [3a. Installing a Virtual Appliance using VMware vCenter \(ISO\)](#).
- **VMware ESXi Stand-Alone Server:** Use [3b. Installing a Virtual Appliance on an ESXi Stand-Alone Server \(ISO\)](#).



Linux KVM has been tested and validated on a number of KVM host versions. Refer to [KVM](#) for a detailed list of the KVM components that we have tested and validated for Secure Network Analytics versions 7.3.1 and above.

Before You Begin

Before you begin the installation, make sure you've completed the following procedures:

1. **Compatibility:** Review the compatibility requirements in [Compatibility](#).
2. **Resource Requirements:** Review the [Resource Requirements](#) section to determine the required allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
3. **Firewall:** Configure your firewall for communications. Refer to [1. Configuring Your Firewall for Communications](#).
4. **Files:** Download the appliance ISO files and copy them to a folder on the KVM host. We use the following folder in the example provided in this section: `var/lib/libvirt/image`. Refer to [2. Downloading Virtual Edition Installation Files](#) for instructions.
5. **Time:** Confirm the time set on the hypervisor host in your VMware environment (where you will be installing the virtual appliance) shows the correct time. Otherwise, the virtual appliances may not be able to boot up.



Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Secure Network Analytics appliances.

Installing a Virtual Appliance on a KVM Host (ISO)

If you have a KVM host, use the following instructions to install a virtual appliance using the ISO.

Process Overview

Installing a virtual appliance involves completing the following procedures, which are covered in this chapter:

Configuring an Isolated LAN for Data Nodes

1. Installing a Virtual Appliance on a KVM Host

2. Adding NIC (Data Node, Flow Sensor) and Promiscuous Port Monitoring on an Open vSwitch (Flow Sensors Only)

Configuring an Isolated LAN for Data Nodes

If you are deploying Data Nodes Virtual Edition to your network, configure an isolated LAN with a virtual switch so that the Data Nodes can communicate with each other over **eth1** for inter-Data Node communication. See your virtual switch's documentation for more information on creating an isolated LAN.

1. Installing a Virtual Appliance on a KVM Host

There are several methods to install a virtual machine on a KVM host using a ISO file. The following steps give one example for installing a virtual Manager through a GUI tool called Virtual Machine Manager running on a Ubuntu box. You can use any compatible Linux distribution. For compatibility details, refer to [Compatibility](#).

Monitoring Traffic

The Flow Sensor Virtual Edition has the ability to provide visibility into KVM environments, generating flow data for areas that are not flow-enabled. As a virtual appliance installed inside each KVM host, the Flow Sensor Virtual Edition passively captures Ethernet frames from traffic it observes and creates flow records containing valuable session statistics that pertain to conversational pairs, bit rates, and packet rates.

Configuration Requirements

This configuration has the following requirements:

- **Promiscuous Mode:** Enabled.
- **Promiscuous Port:** Configured to an open vSwitch.



We recommend that you use virt-manager 2.2.1 to install a virtual appliance on a KVM host.

Installing a Virtual Appliance on a KVM Host

To install a virtual appliance, and enable the Flow Sensor Virtual Edition to monitor traffic, complete the following steps:

1. Use Virtual Machine Manager to connect to the KVM Host and configure the appliance as specified in the following steps.
2. Click **File > New Virtual Machine**.



3. Select **QEMU/KVM** for your connection, and then select **Local install media (ISO image or CDROM)**. Click **Forward**.



4. Click **Browse** to select the appliance image.

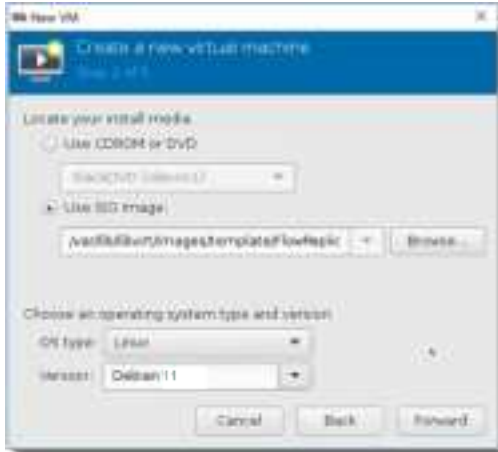


5. Select the ISO file. Click **Choose Volume**.

Confirm the ISO file is accessible by the KVM Host.



6. Deselect the "Automatically detect from the installation media/source" checkbox. Under Choose an operating system type and version, begin typing "Debian" and select the **Debian 11 (debian 11)** option that appears. Click **Forward**.



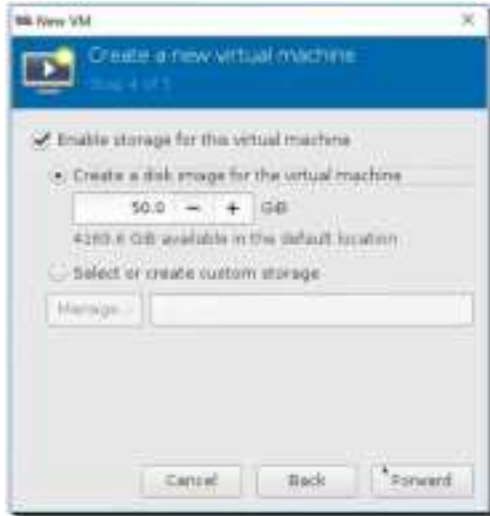
7. Increase the Memory (RAM) and CPUs to the amount shown in the **Resource Requirements** section.

Review [Resource Requirements](#) to allocate sufficient resources. This step is critical for system performance.

⚠ If you choose to deploy Cisco Secure Network Analytics appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.



8. Select **Create a disk image for the virtual machine**.
9. Enter the data storage amount shown for the appliance in the **Resource Requirements** section. Click **Forward**.



Review [Resource Requirements](#) to allocate sufficient resources. This step is critical for system performance.

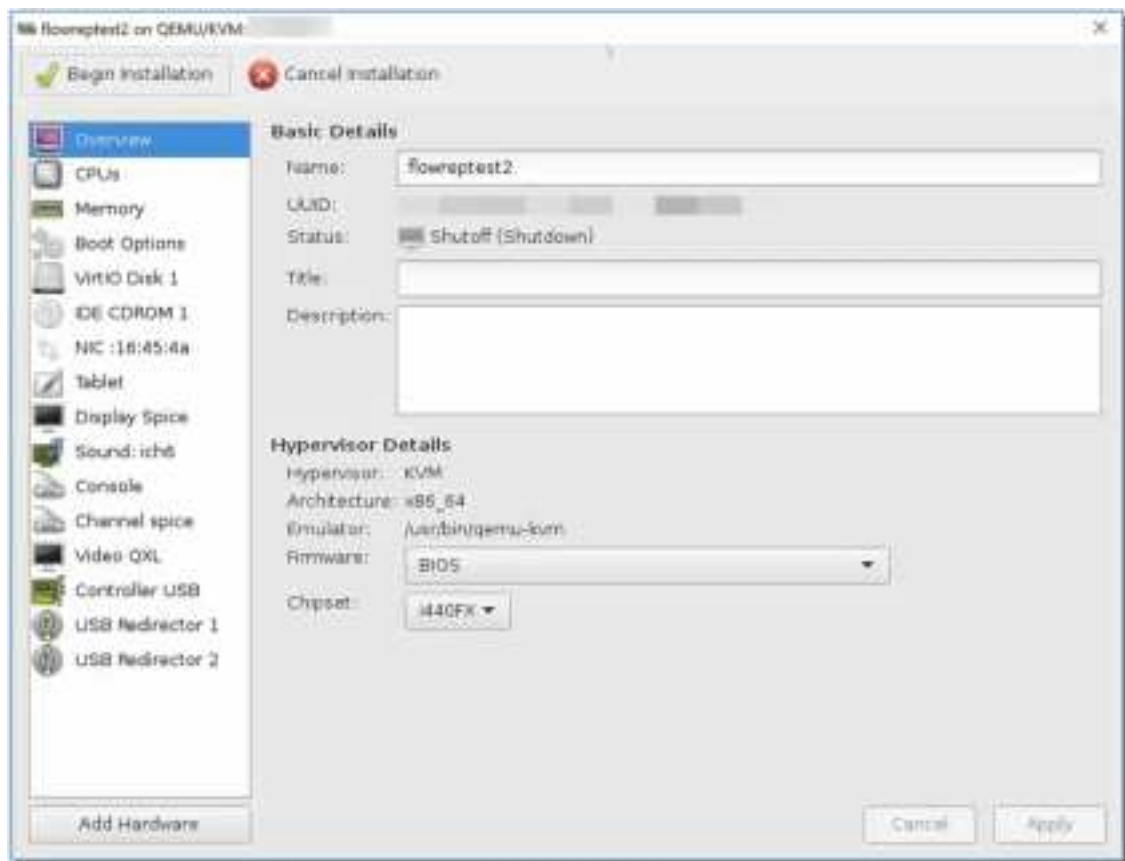
! If you choose to deploy Cisco Secure Network Analytics appliances without the required resources, you assume the responsibility to closely monitor your appliance resource utilization and increase resources as needed to ensure proper health and function of the deployment.

10. Assign a Name for the virtual machine. This will be the display name, so use a name that will help you find it later.
11. Check the **Customize configuration before install** check box.
12. In the **Network selection** drop-down box, select the applicable network and port group for installation.

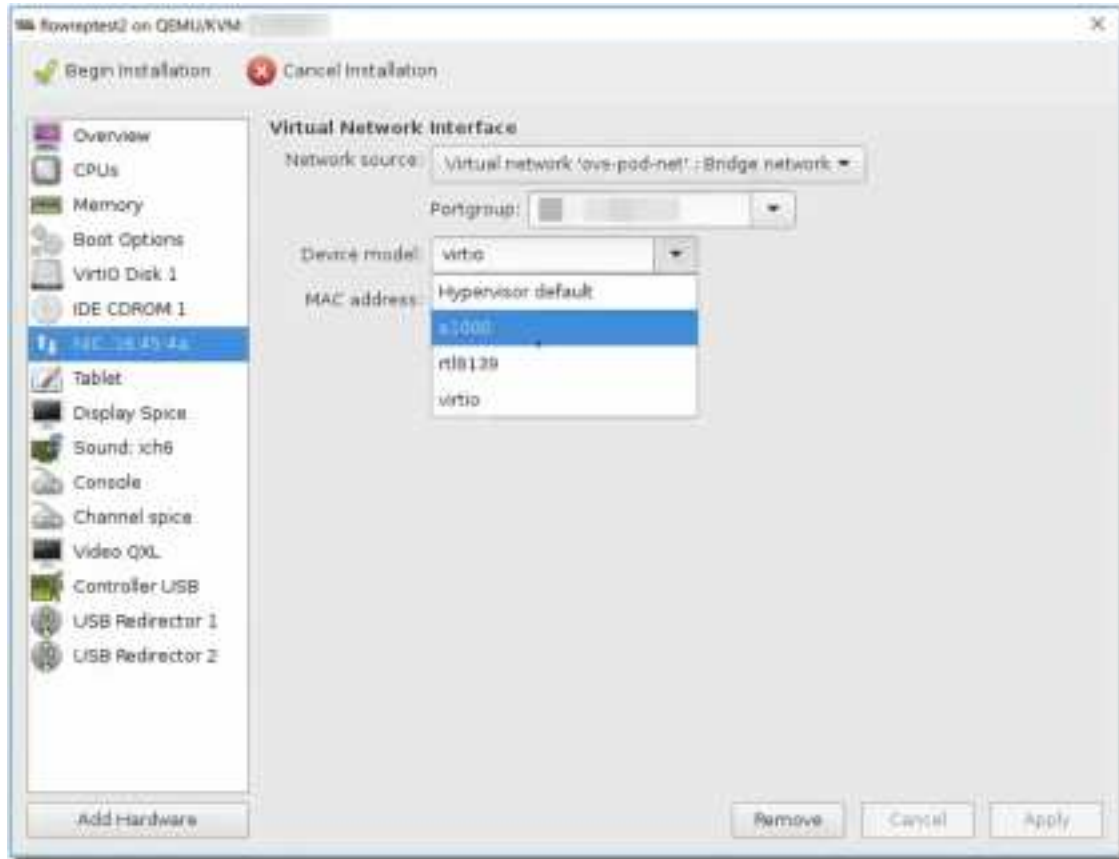
Data Nodes: If this is a Data Node, select a network and port group that will allow the Data Node to communicate on a public network with other appliances.



13. Click **Finish**. The configuration menu opens.



14. In the navigation pane, select **NIC**.
15. Under Virtual Network Interface, select **e1000** in the Device model drop-down box. Click **Apply**.

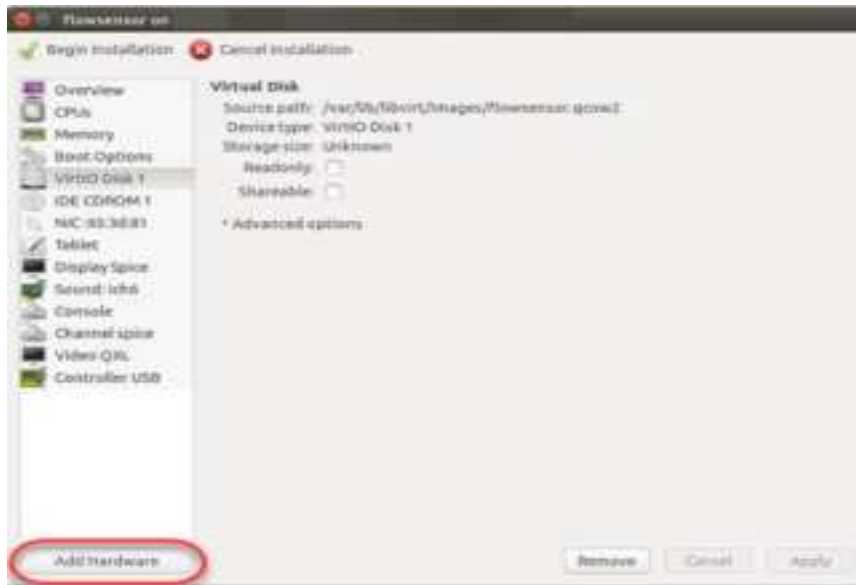


16. Click **VirtIO Disk 1**.
17. In the Advanced Options drop-down list, select **SCSI** in the Disk bus drop-down box. Click **Apply**.
18. Do you need to add additional NICs for monitoring ports on the Flow Sensor Virtual Edition, or to enable inter-Data Node communications on a Data Node VE?
 - If yes, go to [2. Adding NIC \(Data Node, Flow Sensor\) and Promiscuous Port Monitoring on an Open vSwitch \(Flow Sensors Only\)](#).
 - If no, go to the next step.
19. Click **Begin Installation**.
20. Go to [4. Configuring Your Secure Network Analytics System](#).

2. Adding NIC (Data Node, Flow Sensor) and Promiscuous Port Monitoring on an Open vSwitch (Flow Sensors Only)

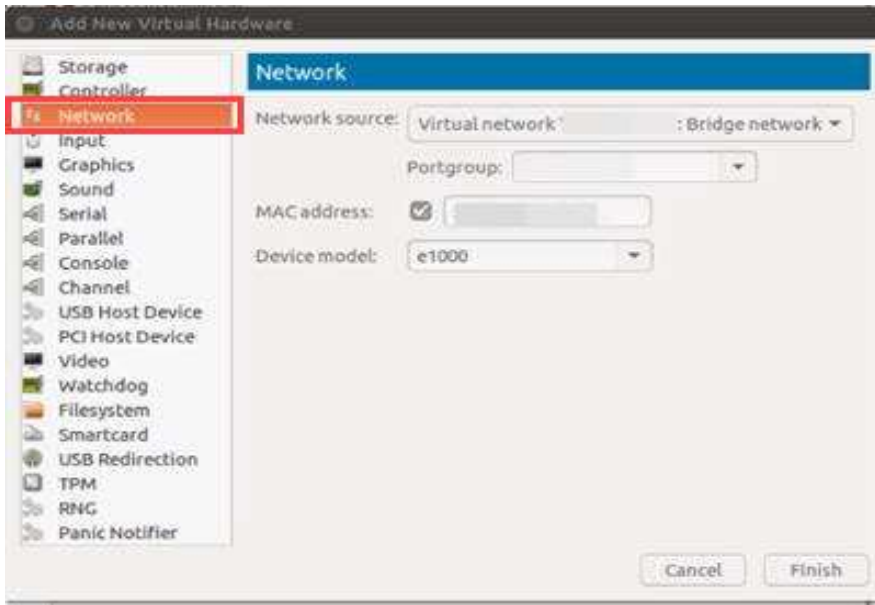
To add additional NICs for the Flow Sensor Virtual Edition monitoring ports or Data Node Virtual Edition and to complete the installation, complete the following steps:

1. In the Configuration Menu, click **Add Hardware**. The Add New Virtual Hardware dialog box displays.



2. In the left navigation pane, click **Network**.

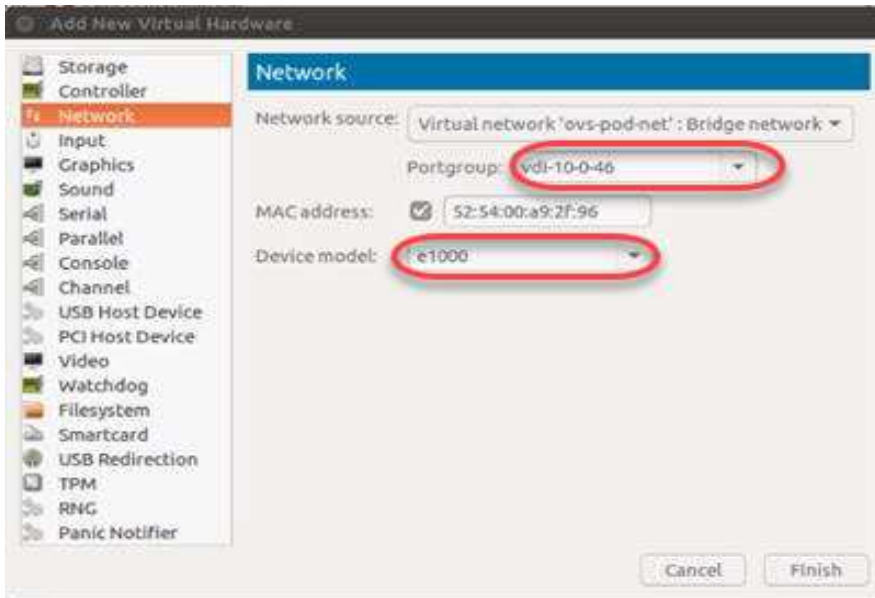
If this is a Data Node, select a network and port group that will allow the Data Node to communicate on a public network with other appliances.



3. **Flow Sensors:** If this is a Flow Sensor, click the Portgroup drop-down list to select an unassigned promiscuous port group you want to monitor.

Click the Device Model drop-down list to select **e1000**.

Data Nodes: If this is a Data Node, select a network source that will allow for inter-Data Node communication on an isolated LAN, using the configuration that you created in [Configuring an Isolated LAN for Data Nodes](#).



4. Click **Finish**.
5. If you need to add another monitoring port, repeat these instructions.
6. After you have added all monitoring ports, click **Begin Installation**.

4. Configuring Your Secure Network Analytics System

If you've finished installing your Virtual Edition appliances and/or hardware appliances, you are ready to configure Secure Network Analytics into a managed system.



To configure Secure Network Analytics, follow the instructions in the [Secure Network Analytics System Configuration Guide v7.4.2](#). This step is critical for the successful configuration and communication of your system.

Make sure you configure your appliances in the order specified in the System Configuration Guide.

System Configuration Requirements

Make sure you have access to the appliance console through the hypervisor host (virtual machine host).

Use the following table to prepare the required information for each appliance.

Configuration Requirement	Details	Appliance
IP Address	Assign a routable IP address to the <code>eth0</code> management port.	
Netmask		
Gateway		
Host Name	A unique host name is required for each appliance. We cannot configure an appliance with the same host name as another appliance. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.	
Domain Name	A fully qualified domain name is required for each appliance. We cannot install an appliance with an empty domain.	

DNS Servers	Internal DNS server for name resolution	
NTP Servers	Internal Time server for synchronization between servers. At least 1 NTP server is required for each appliance. Remove the 130.126.24.53 NTP server if it is in your list of servers. This server is known to be problematic and it is no longer supported in our default list of NTP servers.	
Mail Relay Server	SMTP Mail server to send alerts and notifications	
Flow Collector Export Port	Required for Flow Collectors only. NetFlow Default: 2055	
Non-routable IP Address within a private LAN or VLAN (for inter-Data Node communication)	Required for Data Nodes only. - Hardware eth2 or bond of eth2 and eth3. Creating an LACP <code>eth2/eth3</code> bonded port channel for up to 20G throughput enables faster communication between and among Data Nodes, and quicker Data Node addition or replacement to the Data Store. Note that LACP port bonding is the only bonding option available for hardware Data Nodes. - Virtual eth1 IP Address: You can use the provided IP address or enter a value that meets the following requirements for inter-Data Node communications. Non-routable IP Address from the 169.254.42.0/24 CIDR block,	

	between 169.254.42.2 and 169.254.42.254. • First Three Octets: 169.254.42 • Subnet: /24 • Sequential: For ease of maintenance, select sequential IP addresses (such as 169.254.42.10, 169.254.42.11, and 169.254.42.12). Netmask: The Netmask is hard coded to 255.255.255.0 and cannot be modified.	
eth0 Hardware Connection Port	Required for Secure Network Analytics with Data Store hardware appliances only: • Manager • Flow Collector • Data Nodes eth0 Hardware Connection Port Options: • SFP+:	

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



Change History

Document Version	Published Date	Description
1_0	February 27, 2023	Initial version.
1_1	March 27, 2023	Updated the Communication Ports and Protocols table.
1_2	March 27, 2023	Corrected a typo.
1_3	April 20, 2023	Improved descriptions of VMware support. Removed "Supported Hardware Metrics" table as this is a virtual guide. Improved descriptions of KVM host version support.
1_4	August 15, 2023	Changed memory resource note from GB to GiB.
1_5	April 27, 2023	Added support for VMware 8.0. Revised Deployment recommendations.
1_6	November 16, 2023	Updated the CPU Setting Calculation section.