Copyrights and Trademarks

© 2018 Cisco Systems, Inc. All rights reserved.

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
# CONTENTS

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>About the Flow Sensor VE</td>
<td>1</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>2</td>
</tr>
<tr>
<td>Data Storage</td>
<td>5</td>
</tr>
<tr>
<td>How to Use This Guide</td>
<td>7</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>8</td>
</tr>
<tr>
<td>Installing a Virtual Appliance</td>
<td>9</td>
</tr>
<tr>
<td>Overview</td>
<td>9</td>
</tr>
<tr>
<td>Process Overview</td>
<td>9</td>
</tr>
<tr>
<td>Configuring Your Firewall for Communications</td>
<td>10</td>
</tr>
<tr>
<td>Communication Ports</td>
<td>10</td>
</tr>
<tr>
<td>Integrating the Flow Sensor VE Into Your Network</td>
<td>13</td>
</tr>
<tr>
<td>Placing the Stealthwatch Flow Sensor</td>
<td>13</td>
</tr>
<tr>
<td>Important Considerations for Integration</td>
<td>14</td>
</tr>
<tr>
<td>Installing a Virtual Appliance using VMware vSphere Client</td>
<td>20</td>
</tr>
<tr>
<td>Overview</td>
<td>20</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>20</td>
</tr>
<tr>
<td>Process Overview</td>
<td>20</td>
</tr>
<tr>
<td>Logging in to the VMware vSphere Client</td>
<td>21</td>
</tr>
<tr>
<td>Configuring the Virtual Appliance to Monitor Traffic</td>
<td>21</td>
</tr>
<tr>
<td>Monitoring a vSwitch with Multiple Hosts</td>
<td>21</td>
</tr>
<tr>
<td>Monitoring a vSwitch with a Single Host</td>
<td>26</td>
</tr>
</tbody>
</table>

© 2018 Cisco Systems, Inc. All Rights Reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Virtual Appliance</td>
<td>33</td>
</tr>
<tr>
<td>Defining Additional Monitoring Ports</td>
<td>41</td>
</tr>
<tr>
<td><strong>Installing a Virtual Appliance on a KVM Host</strong></td>
<td>45</td>
</tr>
<tr>
<td>Overview</td>
<td>45</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>45</td>
</tr>
<tr>
<td>Process Overview</td>
<td>45</td>
</tr>
<tr>
<td>Installing a Virtual Appliance on a KVM Host</td>
<td>46</td>
</tr>
<tr>
<td>Adding NIC and Promiscuous Port Monitoring on an Open vSwitch</td>
<td>52</td>
</tr>
<tr>
<td><strong>Configuring the Virtual Environment</strong></td>
<td>55</td>
</tr>
<tr>
<td>Overview</td>
<td>55</td>
</tr>
<tr>
<td>Configure the IP Addresses</td>
<td>55</td>
</tr>
<tr>
<td>Change the Default User Passwords</td>
<td>58</td>
</tr>
<tr>
<td>Changing the sysadmin Password</td>
<td>58</td>
</tr>
<tr>
<td>Changing the root Password</td>
<td>61</td>
</tr>
<tr>
<td><strong>Configuring a Virtual Appliance</strong></td>
<td>65</td>
</tr>
<tr>
<td>Overview</td>
<td>65</td>
</tr>
<tr>
<td>Process Overview</td>
<td>65</td>
</tr>
<tr>
<td>Configuring the Individual Appliances</td>
<td>65</td>
</tr>
<tr>
<td>Expand Data Storage and Resource Allocations</td>
<td>70</td>
</tr>
<tr>
<td>Configuration through the Appliance Admin Interface</td>
<td>72</td>
</tr>
<tr>
<td>Log in to the Appliance Administration Interface</td>
<td>72</td>
</tr>
<tr>
<td>Configure the Advanced Settings</td>
<td>73</td>
</tr>
<tr>
<td>Restart the Virtual Appliance</td>
<td>74</td>
</tr>
</tbody>
</table>
INTRODUCTION

Overview

This is an installation and configuration guide for the Flow Sensor VE in a network.

For Stealthwatch System physical appliances, see the Stealthwatch System Hardware Installation Guide and the Stealthwatch System Hardware Configuration Guide.

Read this chapter to learn more about this guide and how to contact Support, if needed. This chapter includes the following sections:

- Audience
- About the Flow Sensor VE
- Before You Begin
- How to Use This Guide
- Resource Requirements

Audience

The primary audience for this guide is administrators who need to install and configure Stealthwatch Flow Sensor VE appliances. This guide assumes the audience has a basic familiarity with VMware or KVM.

About the Flow Sensor VE

Using the same technology as the Stealthwatch Flow Sensor appliance, the Flow Sensor VE is a virtual appliance that provides visibility into virtual environments, generating flow data for areas that are not flow-enabled.

As a virtual appliance installed inside each virtual host, the Flow Sensor VE connects promiscuously to the virtual switches. You can also configure the Flow Sensor VE to sense traffic on physical network devices just as the physical Flow Sensor does. Once installed, the Flow Sensor VE passively captures Ethernet frames from the traffic it observes and creates flow records containing valuable session statistics that pertain to conversational pairs, bit rates, and packet rates. The Flow Sensor VE then sends these records to any flow collector that supports NetFlow v9.

By directing the Flow Sensor VE toward any NetFlow v9-capable flow collector you can derive valuable detailed traffic statistics from NetFlow. When combined with the Stealthwatch Flow Collector for NetFlow, the Flow Sensor also provides deep insight into
performance metrics and behavioral indicators. These flow performance indicators provide insight into any round-trip latency introduced by the network or by the server-side application.

Because the Flow Sensor VE has packet-level visibility, it can calculate round-trip time (RTT), server response time (SRT), and packet loss for TCP sessions. It includes all of these additional fields in the NetFlow records that it sends to the Stealthwatch Flow Collector for NetFlow.

Before You Begin

Use the information in this section to prepare for installing and configuring the Stealthwatch VE appliances. Note that the configuration is a two-part process using first the VMware vSphere client interface or KVM interface, and then the Appliance Administration (Admin) interface.

Compatibility

You can use VMware vSphere Client v6.x or KVM (Kernel-based Virtual Machine) for the virtual appliance installation. It is important to review the following compatibility information:

VMware vSphere Client v6.x or Later

- **VMware ESX Version**: Stealthwatch VE appliances that are running on older versions of VMware ESX are not compatible with ESX v6.x. If you upgrade VMware to ESX v6.x, you must delete your existing Stealthwatch VE appliances and reinstall them.
- **Live migration** (for example, with vMotion) from host to host is not supported.
- **Virtual machine snapshots** are not supported.

**CAUTION!** Do not install VMware Tools on a Stealthwatch virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

KVM Using 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 3.0.0
  qemu-KVM 2.8.0
  Open vSwitch 2.6.1
  Linux Kernel 4.4.38
  ```
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.

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

Installation Order

It is important to install and configure your virtual appliances in the following order:

1. UDP Director
2. Flow Collector Database 5000 Console (if used)
3. All other Flow Collectors
4. All Flow Sensors
5. Cloud License Concentrator
6. Endpoint Concentrator
7. Secondary Stealthwatch Management Console
8. Primary Stealthwatch Management Console

If you do not follow this recommended order when you set up the Stealthwatch system, the system may not properly collect data from the appliances and you will have to set up each one separately.

CAUTION! Be sure the time setting on the virtual host server (where you will be installing the virtual appliances) reflects the correct time. Otherwise, the appliances may not be able to boot up.

Downloading the VE Software

Before you can complete the procedures in this guide, you must obtain the appliance installation file (OVF or ISO) from the Download and License Center. For instructions on downloading the file for each appliance, see the Downloading and Licensing Stealthwatch Products document in the Download and License Center or on Cisco.com.

Registering and Licensing

As part of the configuration process, you will register and license your Stealthwatch products. For instructions, see the Downloading and Licensing Stealthwatch Products document in the Download and License Center or on Cisco.com.
Resource Requirements

This section provides the resource requirements for the virtual appliances. You can use the tables provided in this section to record settings you will need to install and configure the Stealthwatch VE appliances.

Flow Sensor VE

The Stealthwatch System beginning with v6.9.1 offers various types of Flow Sensor VEs depending upon the number of NICs for the Flow Sensor VE.

The flow cache size adjusts with the amount of reserved memory. Use the flow cache size to calculate the amount of memory needed for the amount of traffic being monitored.

Note: The allocations presented in the table are only recommendations. To achieve desired throughput, any particular environment may require more or less resources and may depend on a number of variables, such as average packet size, burst rate, and other network and host conditions.

<table>
<thead>
<tr>
<th>NICs - monitoring ports (1 GB)</th>
<th>Reserved CPUs</th>
<th>Reserved Memory</th>
<th>Hardware Throughput Equivalent</th>
<th>Flow Cache Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Sensor Base, Flow Sensor VE</td>
<td>1</td>
<td>1</td>
<td>4 GB</td>
<td>N/A</td>
</tr>
<tr>
<td>Flow Sensor Base</td>
<td>4</td>
<td>8</td>
<td>16 GB</td>
<td>Up to FS1200</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>32</td>
<td>32 GB</td>
<td>Up to FS2200</td>
</tr>
</tbody>
</table>

* Interfaces configured as PCI passthrough (igb compliant or e1000e compliant)
Data Storage

During installation, you will expand the available data storage on the server. Use the following information to allocate the correct amount of storage for each appliance.

- **Expansion Calculation**: The virtual appliance uses approximately 75% of the server for data storage, leaving 25% for the operating system and cache. Therefore, always expand the data storage to 40% more than the desired amount.
- **FPS Calculation**: Cisco recommends allocating a minimum of 1 GB of data storage for every 1,000 flows per second (FPS) your system averages daily multiplied by the number of days you want to store the flows. For example, if your system averages 2,000 FPS and you want to store flows for 30 days, allocate a minimum of 60 GB (2 X 30) of data storage space.
- **If the External Event processing (syslog) feature is used**, more memory and processing resources are required.
- **Minimum Data Storage**: Use the following table to determine the minimum data storage required for each appliance.

<table>
<thead>
<tr>
<th>Stealthwatch VE Model</th>
<th>Minimum Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealthwatch Management Console VE</td>
<td>100 GB</td>
</tr>
<tr>
<td>Stealthwatch Management Console VE 2000</td>
<td>200 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE</td>
<td>200 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 2000</td>
<td>600 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 4000</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE</td>
<td>100 GB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 2000</td>
<td>600 GB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 4000</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>50 GB</td>
</tr>
<tr>
<td>UDP Director</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

**Flow Sensor VE**

The Flow Sensor VE requires the connection of a virtual server. For physical server requirements, see your VMware user guide or KVM user guide.
Flow Sensor VE Network Environments

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

**Note:** Stealthwatch supports a VDS environment, but it does not support VMware Distributed Resource Scheduler (VM-DRS).

The Flow Sensor VE 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

Information Needed for Console Access

<table>
<thead>
<tr>
<th>Setting</th>
<th>Hypervisor Server</th>
<th>Flow Sensor VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login User Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td>(Default = 192.168.1.6)</td>
</tr>
<tr>
<td>Netmask IP Address</td>
<td></td>
<td>(Default = 255.255.255.0)</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td></td>
<td>(Default = 192.168.1.1)</td>
</tr>
</tbody>
</table>

Information Needed for the Appliance Admin Interface

<table>
<thead>
<tr>
<th>Setting</th>
<th>Flow Sensor VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>(Default = 192.168.1.6)</td>
</tr>
<tr>
<td>Host Name</td>
<td></td>
</tr>
<tr>
<td>Network Domain Name</td>
<td></td>
</tr>
<tr>
<td>NTP Server IP Address(es)</td>
<td></td>
</tr>
<tr>
<td>DNS Server IP Address(es)</td>
<td></td>
</tr>
</tbody>
</table>

The Flow Sensor VE requires the following additional information:
IP addresses and listening port numbers (default = 2055) for each NetFlow collector and/or UDP Director™ that will be receiving data from the Flow Sensor VE

How to Use This Guide

In addition to this introduction, we have divided this guide into the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing a Virtual Appliance</td>
<td>How to prepare the virtual environment and install VE appliances</td>
</tr>
<tr>
<td>Configuring the Virtual Environment</td>
<td>How to set up the virtual environment for the appliances</td>
</tr>
<tr>
<td>Configuring a Virtual Appliance System</td>
<td>How to configure appliances to begin processing traffic data</td>
</tr>
</tbody>
</table>

Abbreviations

The following abbreviations may appear in this guide:

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Domain Name System (Service or Server)</td>
</tr>
<tr>
<td>dvPort</td>
<td>Distributed Virtual Port</td>
</tr>
<tr>
<td>ESX</td>
<td>Enterprise Server X</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-based Virtual Machine</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OVF</td>
<td>Open Virtualization Format</td>
</tr>
<tr>
<td>SMC</td>
<td>Stealthwatch Management Console</td>
</tr>
<tr>
<td>TB</td>
<td>Terabyte</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>UUID</td>
<td>Universally Unique Identifier</td>
</tr>
<tr>
<td>VDS</td>
<td>vNetwork Distributed Switch</td>
</tr>
<tr>
<td>VE</td>
<td>Virtual Edition</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
</tbody>
</table>

**Contacting Support**

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

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch Support
  - To open a case by email: tac@cisco.com
  - For phone support: 1-800-553-2447 (U.S.)
INSTALLING A VIRTUAL APPLIANCE

Overview

This chapter describes how to install the virtual appliances.

For instructions on how to install a Stealthwatch physical appliance, see the Stealthwatch System v6.x Hardware Installation Guide.

Compatibility: You can use one of the following for the virtual edition installation. For compatibility details, see the Compatibility section of the Introduction.

- VMware vSphere Client v6.x or later
- KVM using any Linux distribution

**Note**: Confirm the time setting on the virtual host server (where you will be installing the virtual appliances) reflects the correct time. Otherwise, the appliances may not be able to boot up.

**CAUTION!** Do not install VMware Tools on a Stealthwatch virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

Process Overview

Installing a virtual appliance involves completing the following procedures, which we discuss in this chapter:

1. Configuring Your Firewall for Communications
2. Integrating the Flow Sensor VE Into Your Network
3. Installing a Virtual Appliance using VMware vSphere Client or KVM.
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.

Consult with your network administrator to ensure that the following ports are open and have unrestricted access:

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Communication Ports

The following table shows how the ports are used in the Stealthwatch System:

<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin User PC</td>
<td>All appliances</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>All appliances</td>
<td>Network time source</td>
<td>UDP/123</td>
<td>NTP</td>
</tr>
<tr>
<td>Active Directory</td>
<td>SMC</td>
<td>TCP/389, UDP/389</td>
<td>LDAP</td>
</tr>
<tr>
<td>AnyConnect</td>
<td>Endpoint Concentrator</td>
<td>UDP/2055</td>
<td>NetFlow</td>
</tr>
<tr>
<td>From (Client)</td>
<td>To (Server)</td>
<td>Port</td>
<td>Protocol</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>Cisco ISE</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Cisco ISE</td>
<td>SMC</td>
<td>TCP/5222</td>
<td>XMPP</td>
</tr>
<tr>
<td>Endpoint Concentrator</td>
<td>Flow Collector</td>
<td>UDP/2055</td>
<td>NetFlow</td>
</tr>
<tr>
<td>External log sources</td>
<td>SMC</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>Flow Collector</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SLIC</td>
<td>SMC</td>
<td>TCP/443 or proxied connection</td>
<td>HTTPS</td>
</tr>
<tr>
<td>UDP Director</td>
<td>Flow Collector - sFlow</td>
<td>UDP/6343</td>
<td>sFlow</td>
</tr>
<tr>
<td>UDP Director</td>
<td>Flow Collector - NetFlow</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>UDP Director</td>
<td>3rd Party event management systems</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Identity</td>
<td>SMC</td>
<td>TCP/2393</td>
<td>SSL</td>
</tr>
<tr>
<td>NetFlow Exporters</td>
<td>Flow Collector - NetFlow</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>sFlow Exporters</td>
<td>Flow Collector - sFlow</td>
<td>UDP/6343*</td>
<td>sFlow</td>
</tr>
<tr>
<td>SMC</td>
<td>Cisco ISE</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>DNS</td>
<td>UDP/53</td>
<td>DNS</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Collector</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>From (Client)</td>
<td>To (Server)</td>
<td>Port</td>
<td>Protocol</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Sensor</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>Identity</td>
<td>TCP/2393</td>
<td>SSL</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Exporters</td>
<td>UDP/161</td>
<td>SNMP</td>
</tr>
<tr>
<td>SMC</td>
<td>Endpoint Concentrator</td>
<td>UDP.2055</td>
<td>HTTPS</td>
</tr>
<tr>
<td>User PC</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>All appliances</td>
<td>User PC</td>
<td>TCP/22</td>
<td>SSH</td>
</tr>
<tr>
<td>SMC</td>
<td>3rd Party event management systems</td>
<td>UDP/162</td>
<td>SNMP-trap</td>
</tr>
<tr>
<td>SMC</td>
<td>3rd Party event management systems</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>SMC</td>
<td>Email gateway</td>
<td>TCP/25</td>
<td>SMTP</td>
</tr>
<tr>
<td>SMC</td>
<td>SLIC</td>
<td>TCP/443</td>
<td>SSL</td>
</tr>
<tr>
<td>User PC</td>
<td>All appliances</td>
<td>TCP/22</td>
<td>SSH</td>
</tr>
</tbody>
</table>

The following diagram shows the various connections used by the Stealthwatch System. The ports marked as *optional* may be used according to your own network needs.
Integrating the Flow Sensor VE Into Your Network

The Flow Sensor VE has the ability to provide visibility into your network as a passive monitoring device. It can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

Placing the Stealthwatch Flow Sensor

The Flow Sensor VE appliance is most effective when placed at critical segments of your corporate network as follows:
- **Inside your firewall** to monitor traffic and determine if a firewall breach has occurred
- **Outside your firewall**, monitoring traffic flow to analyze who is threatening your firewall
- **At sensitive segments of your network**, offering protection from disgruntled employees or hackers with root access
- **At remote office locations** that constitute vulnerable network extensions
- **On your business network for protocol use management** (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers’ financial data)

### Important Considerations for Integration

The Stealthwatch Flow Sensor VE is versatile enough to integrate with a wide variety of network topologies, technologies, and components. Before you install a Flow Sensor VE, you must make several decisions about your network and how you want to monitor it. It is important to review the following:

- Analyze your network's topology and your specific monitoring needs.
- Connect a Flow Sensor so that it receives network transmissions to and from the monitored network, and, if desired, receives interior network transmissions as well.
- For optimum performance when using the Flow Sensor to monitor physical network traffic, configure your Flow Sensor VE with direct access to the underlying physical host’s NICs (such as using an igb or e1000e compliant PCI pass-through).

The following sections explain how to integrate a Stealthwatch Flow Sensor VE appliance into your network using the following Ethernet network devices:

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

**Note:** While not all network configurations can be discussed here, the examples may help you determine the best setup for your monitoring needs. These examples provide physical network scenarios, and the virtual host can be configured in a similar way.

### TAPs

When a Test Access Port (TAP) is placed *in line* with a network connection, it repeats the connection on a separate port or ports. For example, an Ethernet TAP placed in line with an Ethernet cable will repeat each direction of transmission on separate ports. Therefore, use of a TAP is the most reliable way to use the Flow Sensor. The type of TAP you use depends on your network.

For important configuration information, see [Configure the Advanced Settings](#) in the Configuring a Virtual Appliance chapter.

This section explains the following ways to use TAPs:
- Using Electrical TAPs
- Using Optical TAPs
- Using TAPs Outside Your Firewall
- Placing the Flow Sensor VE Inside Your Firewall

**Note:** In a network using TAPs, the Flow Sensor VE can capture performance monitoring data only if it is connected to an aggregating TAP that is capturing both inbound and outbound traffic. If the Flow Sensor VE is connected to a unidirectional TAP that is capturing only one direction of traffic on each port, then the Flow Sensor VE will not capture performance monitoring data.

### Using Electrical TAPs

The following illustration shows the Stealthwatch Flow Sensor VE connected to an Ethernet electrical TAP. To achieve this configuration, connect the two TAP ports to the Flow Sensor VE Monitor Ports 1 and 2, as shown.

![Using Electrical TAPs Diagram](image)

### Using Optical TAPs

Two splitters are required for fiber-optic-based systems. You can place a fiber-optic cable splitter in line with each direction of transmission and use it to repeat the optical signal for one direction of transmission.

The following illustration shows the Flow Sensor connected to a fiber-optic-based network. To achieve this configuration, connect the outputs of the optical splitters to the Flow Sensor VE Monitor Ports 1 and 2, as shown.
**Note:** If the connection between the monitored networks is an optical connection, then the Stealthwatch Flow Sensor VE appliance is connected to two optical splitters. The management port is connected to either the switch of the monitored network or to another switch or hub.

**Using TAPs Outside Your Firewall**

To have the Flow Sensor VE monitor traffic between your firewall and other networks, connect the Stealthwatch management port to a switch or port outside of the firewall.

**WARNING!** Cisco strongly recommends that you use a TAP for this connection so that failure of the device does not bring down your entire network.

The following illustration shows an example of this configuration using an Ethernet electrical TAP. The management port must be connected to the switch or hub of the monitored network. This setup is similar to the setup that monitors traffic to and from your network.

**Note:** If your firewall is performing network address translation (NAT), you can observe only the addresses that are on the firewall.
Placing the Flow Sensor VE Inside Your Firewall

To monitor traffic between internal networks and a firewall, the Flow Sensor VE must be able to access all traffic between the firewall and the internal networks. You can accomplish this by configuring a mirror port that mirrors the connection to the firewall on the main switch. Make sure that the Flow Sensor VE Monitor Port 1 is connected to the mirror port, as shown in the following illustration:

![Diagram showing how to place the Flow Sensor VE inside a firewall](image)

To monitor traffic inside your firewall by using a TAP, insert the TAP or optical splitter between your firewall and the main switch or hub. A TAP configuration is shown below.

![Diagram showing TAP configuration](image)

An optical splitter configuration is shown below.

![Diagram showing optical splitter configuration](image)
SPAN Ports

You can also connect the Flow Sensor VE to a switch. However, because a switch does not repeat all traffic on each port, the Flow Sensor VE will not perform properly unless the switch can repeat packets transmitted to and from one or more switch ports. This type of switch port is sometimes called a mirror port or Switch Port Analyzer (SPAN).

The following illustration shows how you can achieve this configuration by connecting your network to the Stealthwatch Flow Sensor VE through the management port.

In this configuration, you must configure a switch port (also called a mirror port), to repeat all traffic to and from the host of interest to the mirror port. The Flow Sensor VE Monitor Port 1 must be connected to this mirror port. This allows the Flow Sensor to monitor traffic to and from the network of interest and to other networks. In this instance, a network may be made up of some or all of the hosts connected to the switch.

A common way of configuring networks on a switch is to zone them into virtual local area networks (VLANs), which are logical rather than physical connections of hosts. If the mirror port is configured to mirror all ports on a VLAN or switch, the Flow Sensor VE can monitor all traffic to, from, and within the network of interest, as well as other networks.
For important configuration information, see Configure the Advanced Settings in the "Configuring a Virtual Appliance" chapter.

**Note:** In all cases, Cisco recommends that you consult your switch manufacturer’s documentation to determine how to configure the switch mirror port and what traffic will be repeated to the mirror port.

**Note:** Go to the section that is applicable to your virtual appliance installation: VMware vSphere Client or KVM.
INSTALLING A VIRTUAL APPLIANCE USING VMWARE VSHERE CLIENT

Overview

This chapter describes how to install the virtual appliances using VMware vSphere Client v6.

Before You Begin

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

1. Download the OVF file from the Download and License Center. See the Downloading and Licensing Guide for instructions.
2. Review the Compatibility information in the Introduction.
3. Configure Your Firewall for Communications.
4. Review the Resource Requirements section to determine the proper allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
5. Confirm the time set on the ESX server (where you will be installing the virtual appliance) reflects the correct time. Otherwise, the virtual appliances may not be able to boot up.

WARNING! Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Stealthwatch System appliances.

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

Process Overview

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

1. Logging in to the VMware vSphere Client
2. Configuring the Virtual Appliance to Monitor Traffic
3. Installing the Virtual Appliance
4. Defining Additional Monitoring Ports

© 2018 Cisco Systems, Inc. All Rights Reserved.
Logging in to the VMware vSphere Client

To install the virtual appliance, you must first log in to the VMware vSphere Client v6.x, by completing the following steps:

**Note:** Whether you are using the The VMware vSphere Client or Web Client interface, some of the graphics and commands may vary from the information shown here. Please see your VMware vSphere guide for details related to the software.

1. Launch the VMware vSphere Client software. The Login dialog opens.

2. Type the IP address of the ESX server and your login credentials.
3. Click *Login*. The Home page opens.

Configuring the Virtual Appliance to Monitor Traffic

The Flow Sensor VE 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 vSphere/ESX host, the Flow Sensor VE 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. For details, see *Installing a Virtual Appliance: Integrating the Flow Sensor VE into your network.*

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

- Monitoring a vSwitch with Multiple Hosts
- Monitoring a vSwitch with a Single Host

**Monitoring a vSwitch with Multiple Hosts**

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

© 2018 Cisco Systems, Inc. All Rights Reserved.
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.

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 VE will monitor. If the Flow Sensor VE 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 will 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. In the View menu, select Inventory > Networking to display the Networking tree on the left.

   ![Networking menu screen](image1)

   On the Web client, click Networking in the Inventory Tree list:

   ![Networking menu on Web client](image2)

2. In the Networking tree, select the VDS.
3. In the right pane, click **Create a new port group**.

The Create dvPort Group wizard opens.

**Note:** The Web Client has two dialogs for the configuration: Select name and location and Configure settings.
4. In the Name field, type the name you want to use to identify this dvPort group.

5. In the Number of Ports field, type the number of Flow Sensor VE{s} in your cluster of hosts.

6. Does your environment use a VLAN?
   - If yes, select the VLAN type from the drop-down list. Then, go to Step 7.
   - If no, select None from the VLAN type drop-down list. Then, go to step 8.

7. Based on the VLAN type you selected, perform the action indicated in the following table:

<table>
<thead>
<tr>
<th>VLAN Type</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>In the VLAN ID field, enter the number (between 1 and 4094) that matches the identifier.</td>
</tr>
<tr>
<td>VLAN Trunking</td>
<td>In the VLAN trunk range field, enter 0-4094 to monitor all VLAN traffic.</td>
</tr>
<tr>
<td>Private VLAN</td>
<td>Select Promiscuous from the drop-down list.</td>
</tr>
</tbody>
</table>

8. Click Next. A Summary page opens.

10. Right-click the new dvPort group. Select **Edit Settings**.

The Settings dialog opens.

11. In the left pane, select **Security**.
12. In the right pane in the Promiscuous Mode drop-down list, select **Accept**.
13. Click **OK** to close the dialog.
14. Does the Flow Sensor VE 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.

15. Is there another VDS on the ESX server that the Flow Sensor VE will monitor?
If yes, repeat the steps in this section Monitoring a vSwitch with Multiple Hosts for the next VDS.
If no, go to Installing the Virtual Appliance.

Monitoring a vSwitch with a Single Host

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

Note: This section applies only to non-VDS networks. If your network uses a VDS, go to Monitoring a vSwitch with Multiple Hosts.

This configuration has the following requirements:

- **Promiscuous Port Group**: Add a promiscuous port group for each virtual switch that the Flow Sensor VE will be monitoring.
- **Promiscuous Mode**: enabled
- **Promiscuous Port**: configured to the vSwitch

Complete the following steps to configure the network using a non-VDS environment.

1. Add a Port Group
2. Set the Port Group to Promiscuous Mode

Add a Port Group

To add a port group, complete the following steps:

1. In the Inventory tree, select the ESX server, and then click the Configuration tab.
The Configuration page opens.

2. In the Hardware pane, click **Networking**.

   The Configuration tab displays the list of installed virtual switches.
3. Scroll through the list to locate the virtual switch that the Flow Sensor VE will be monitoring, and then click the **Properties** link. The Properties dialog for that virtual switch opens.

![Properties dialog](image)

4. Click **Add**. The Add Network Wizard opens to the Connection Type page.

![Add Network Wizard](image)
5. Under **Connection Types**, select **Virtual Machine**. Click **Next**. The Connection Settings page opens.

6. **Optional:** Change the **Network Label** for the port group.

7. Click the **VLAN ID** drop-down list and select **All (4095)** to allow the Flow Sensor VE to see traffic on all VLANs through this port group.

8. Click **Next**. The Summary page opens, showing the port group you added.
9. Click **Finish** to return to the virtual switch Properties dialog, which shows the new port group.

10. Continue with the next section.
Set the Port Group to Promiscuous Mode

To set the port group to Promiscuous Mode, complete the following steps:

1. On the virtual switch Properties dialog, select the port group you just added and click **Edit**.

   ![Properties dialog for port group](image1.png)

   The Properties dialog for the port group opens.

2. Click the **Security** tab to display the **Policy Exceptions** options.

   ![VM Network 3 Properties](image2.png)
3. Click the **Promiscuous Mode** checkbox. Select **Accept** from the drop-down list.
4. Click **OK** to return to the virtual switch Properties dialog.
5. Click **Close** to dismiss the virtual switch Properties dialog. The new port group appears on the Networking page of the Configuration tab.
6. Will the Flow Sensor VE be monitoring another virtual switch on this ESX server?
   - If yes, go back to Configuring the Virtual Appliance to Monitor Traffic, and repeat all the steps for the next virtual switch.
   - If no, continue with the next section, Installing the Virtual Appliance.

Installing the Virtual Appliance

To install a virtual appliance on the ESX server and define the virtual appliance management and monitoring ports, complete the following steps:

1. Locate the virtual appliance software file (OVF.TGZ) that you downloaded from the Download and License Center.
2. Unzip or open the file, and then untar it.
   - To untar the file, select all the files in the folder and extract them.
   - Unzipping TGZ file is a two-step process, and the steps may vary depending on the software you use.

3. On the vSphere client menu, click File > Deploy OVF Template.
   Web Client: Right-click the host. Select Deploy OVF Template.

Note: The Web client OVF template wizard may vary from the images and instructions shown here, but the steps are similar. One example is the Web client uses Source Location instead of Source. The image below shows the steps on the left side for a OVF template ready to deploy:
The Deploy OVF Template wizard opens.

4. Click **Browse**. Navigate to select the virtual appliance OVF file.
5. Click **Next** to display the OVF Template Details page.

**Web Client:** The 1.b. Review details page opens.
6. Click **Next**. Review the End User License Agreement.

   **Web Client:** 1c. Accept EULAs.

7. After reviewing the information, click **Accept**. Click **Next**. The Name and Location page opens.

   **Web Client:** 2a. The Name and Location page opens.
8. **Optional**: Change the name and location for the virtual appliance. This should be a unique name and will display in the Inventory tree. Click **Next**.

9. On the Storage page, select where you want to store the data files. Click **Next**.
10. On the Disk Format page, select **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed**. Click **Next**.
   - Use the Thin Provision format only if your disk space is limited.
   - For more information, see your VMware documentation.
11. On the Network Mapping page, select the networks for the virtual appliance. Click **Next**.

**Web Client:** The 2c. Setup Networks page opens.
12. On the Ready to Complete page, review the summary of settings. If they are correct, click Finish.
13. The deployment dialog box opens.

14. When the deployment is completed, click **Close**. The installed virtual appliance appears in the Inventory tree.

15. Are you installing a Flow Sensor VE, which will be monitoring more than one virtual switch on an ESX server or more than one VDS in a cluster?
   - If yes, continue with the next section, **Defining Additional Monitoring Ports**.
   - If no, go to **Configuring the Virtual Environment**
Defining Additional Monitoring Ports

**Note:** This procedure is necessary **only** if the Flow Sensor VE will be monitoring more than one virtual switch on an ESX server or more than one VDS in a cluster.

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

1. In the Inventory tree, right-click the Flow Sensor VE, and then select **Edit Settings**.

2. Click **Add**. The Add Hardware dialog opens to the Device Type page.

3. Select **Ethernet Adapter** in the list of device types, and then click **Next**. The Network Type page opens.
4. Do the following:
   - In the **Adapter Type** section, select **VMXNET 3**.
   - In the **Network Connection** section, select an unassigned promiscuous port group.
   - In the **Device Status** section, make sure that the **Connect at power on** check box is selected.

5. Click **Next** to see a summary.
6. After reviewing the settings, click Finish.
7. The Flow Sensor VE Virtual Machine Properties dialog opens, showing the newly defined monitor port.

8. Will the Flow Sensor VE be monitoring another virtual switch on the ESX server or another VDS in a cluster?
   - If yes, repeat this procedure for the next virtual switch.
   - If no, click OK to return to the vSphere Client Home page.

9. Go to Configuring the Virtual Environment
INSTALLING A VIRTUAL APPLIANCE ON A KVM HOST

Overview

This chapter describes how to install the virtual appliances using KVM and Virtual Machine Manager.

Before You Begin

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

1. Download the ISO file from the Download and License Center and copy the image to a folder on the KVM host. In the example given below, the folder is var/lib/libvirt/image. See the Downloading and Licensing Guide for instructions.
2. Review the Compatibility information in the Introduction.
3. Configure Your Firewall for Communications.
4. Review the Resource Requirements section to determine the proper allocations for the appliance.
5. Confirm the time set on the virtual host server (where you will be installing the virtual appliance) reflects the correct time. Otherwise, the virtual appliances may not be able to boot up.

WARNING! Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Stealthwatch System appliances.

Process Overview

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

- Installing a Virtual Appliance on a KVM Host
- Adding NIC and Promiscuous Port Monitoring on an Open vSwitch
Installing a Virtual Appliance on a KVM Host

There are several methods to install a virtual machine on a KVM host using an ISO file. The following steps give one example for installing a virtual SMC appliance through a GUI tool called Virtual Machine Manager running on a Ubuntu box. You can use any compatible Linux distribution. For compatibility details, see the Compatibility section of the Introduction.

Monitoring Traffic: The Flow Sensor VE 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 VE 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. For details, see Installing a Virtual Appliance: Integrating the Flow Sensor VE into your network.

This configuration has the following requirements, which is covered in this chapter:

- **Promiscuous Mode**: enabled
- **Promiscuous Port**: configured to an open vSwitch

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

1. Use Virtual Machine Manager to connect to the KVM Host.
2. Click **File > New Virtual Machine**.
3. Select **Local install media (ISO image or CDROM)**, and then click **Forward**.
4. Click **Use ISO image**.
5. Click **Browse**. Select the appliance image.

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

**Note:** Confirm the ISO file is accessible by the KVM Host.
7. Under Choose an operating system type and version, select **Linux** from the OS type drop-down list.

8. From the Version drop-down list, select **Debian Jessie**. Click **Forward**.

9. Increase the Memory (RAM) and CPUs to the amount shown in the Resource Requirements section.
10. Click **Forward**.
11. Select **Create a disk image for the virtual machine**.
12. Enter the data storage amount shown for the appliance in the Resource Requirements section. Click **Forward**.

13. Assign a Name for the virtual machine. This will be the display name, so use a name that will help you find it later.

14. Select the **Customize configuration before install** check box.
15. In the Network selection drop-down box, select the applicable network and port group for installation.
16. Click Finish. The configuration menu opens.
17. In the navigation pane, select **NIC**.
18. Under Virtual Network Interface, select **e1000** in the Device model drop-down box. Click **Apply**.

![Image of virtual network interface configuration]

19. Click **VirtIO Disk 1**.
20. In the Advanced Options drop-down list, select **SCSI** in the Disk bus drop-down box. Click **Apply**.
21. Do you need to add additional NICS for monitoring ports on the Flow Sensor VE?
   - If yes, go to **Adding NIC and Promiscuous Port Monitoring on an Open vSwitch**.
   - If no, go to the next step.

21. Click **Begin Installation**.
22. Go to **Configuring the Virtual Environment**.
Adding NIC and Promiscuous Port Monitoring on an Open vSwitch

To add additional NICs for the Flow Sensor VE monitoring ports and to complete the installation, complete the following steps:

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

2. In the left navigation pane, click **Network**.
3. 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**.

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**.
CONFIGURING THE VIRTUAL ENVIRONMENT

Overview

After you install the Stealthwatch VE appliances, you are ready to configure the virtual environment for them. This process involves completing the following procedures as detailed in this chapter:

1. Configure the IP Addresses
2. Change the Default User Passwords

Configure the IP Addresses

To configure the IP addresses for a virtual appliance, complete the following steps:

1. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Confirm the virtual machine is powered on.

Note: If the virtual machine does not power on and you receive an error message about insufficient available memory, do one of the following:

- Increase the available resources on the system where the appliance is installed. See the Resource Requirements section for details.
- ESX server: Increase the memory reservation limit for the appliance and its resource pool.

4. Access the virtual machine console.
5. Allow the virtual appliance to finish booting up. The virtual appliance Administrative IP Address page opens.

Note: You may need to enable the Full Screen Mode to view the entire screen.
6. Click on the page. Enter the IP address for the virtual appliance.
7. Select OK, and then press Enter. The IP Netmask page opens with the default network mask IP address.

8. Do the following:
   - Accept the default value or enter a new one based on your environment.
   - Select OK and press Enter to continue.

The IP Broadcast Address page opens with the default broadcast IP address.

9. Do the following:
   - Accept the default value or enter a new one based on your environment.
   - Select OK and press Enter to continue.

The Gateway Address page opens with the default gateway server IP address.
10. Do the following:
   
   - Accept the default value or enter a new one based on your environment.
   - Select OK and press Enter to continue.

   A page opens showing a summary of your entries.

11. Review the information. Are the settings correct?
   
   - If yes, go to the next step.
   - If no, go to step 13.

12. Press Enter. The system restart page opens.
13. Press **Enter**. The system restarts and implements the changes. On completion, a login prompt appears.

14. Select **No** and press **Enter**. The Administrative IP Address page opens. Repeat steps 5 through 10 to make any necessary changes. The system restart page opens.

15. Press **Enter**. The system restarts and implements the changes. On completion, a login prompt appears.

16. Press **Ctrl + Alt** to exit the console.

17. Go to Change the Default User Passwords next in this chapter.

---

### Change the Default User Passwords

**Important:** To ensure that your network is secure, you must change the default password for the sysadmin and root users.

#### Changing the sysadmin Password

To change the sysadmin password, complete the following steps:
1. At the login page, do the following:
   
   a. Type **sysadmin** (case-sensitive), and then press **Enter**.
   b. When the password prompt appears, type **lan1cope**, and then press **Enter**.

2. On the System Configuration menu, select **Password** and press **Enter**.

   ![](image1.png)

   **Important:** If you change the trusted hosts list from the defaults, you must make sure each Stealthwatch appliance is included in the trusted host list for every other Stealthwatch appliance in your deployment. Otherwise, the appliances will not be able to communicate with each other.

   A prompt for the current password appears below the menu.

   ![](image2.png)

3. Type the current password, and then press **Enter**.

   The prompt for a new password appears.
4. Type the new password, and then press Enter.

**Notes:**
- The password must be between 8 and 30 alphanumeric characters in length with no spaces. You also may use the following special characters: $.~!@#%_=?:,{}
- Any password change must be different from the previous password by at least four characters.

5. Type the new password again, and then press Enter. A message appears indicating that the password was updated successfully.

6. Press Enter to return to the System Configuration Console menu.
7. Continue with the next section, “Changing the root Password.”
Changing the root Password

To change the root password, complete the following steps:

1. On the System Configuration Console menu, select Advanced, and then press Enter. The Advanced menu opens.

2. On the Advanced menu, select RootShell, and then press Enter.

A prompt for the root password appears.

3. Type the current root password, lan1cope, and then press Enter. The root shell prompt appears.
4. Type **SystemConfig** (case-sensitive), and then press **Enter**.

   This returns you to the System Configuration menu so that you can change the root password.

5. Select **Password**, and then press **Enter**. The password prompt appears.

6. Type the new root password, and then press **Enter**. A second prompt appears below the menu.

7. Retype the new root password, and then press **Enter**.
A message appears indicating that the password was updated successfully.

8. When your password change is successful, type `exit`, and then press `Enter`. You have now changed both of your default sysadmin and root passwords.

9. Press `Ctrl+Alt` to exit the console environment.

10. Have you completed all of the procedures in this chapter for all of the virtual appliances?
    
    - If yes, continue with Configuring a Virtual Appliance System.
    - If no, return to Configure the IP Addresses and repeat all of the procedures in this chapter for the next virtual appliance. Then, go to the Configuring a Virtual Appliance.
CONFIGURING A VIRTUAL APPLIANCE

Overview

This chapter provides the procedures for configuring the virtual appliance to begin processing traffic data. Once you have completed the steps in this chapter, the installation and configuration process is complete.

Note: Please refer to the checklist on “Before You Begin” on page 2 for the information you will need before proceeding.

Process Overview

Configuring a virtual Stealthwatch appliance involves completing the following procedures, which we discuss in this chapter:

1. Configuring the Individual Appliances
2. Expand Data Storage and Resource Allocations
3. Configuration through the Appliance Admin Interface

Configuring the Individual Appliances

Initial configuration of every appliance is done with the Appliance Setup Tool. The first time you access the appliance, the Appliance Setup Tool is displayed.

It is important to install and configure your virtual appliances in the following order:

1. UDP Director VE
2. Flow Collector Database 5000 Console (if used)
3. All other Flow Collectors
4. All Flow Sensors
5. Cloud License Concentrator
6. Endpoint Concentrator
7. Secondary Stealthwatch Management Console
8. Primary Stealthwatch Management Console

Before you begin, gather the information detailed in the “Before You Begin” on page 2.

**Note:** Your screens may look slightly different from the ones presented here depending on your environment.

To configure an appliance, complete the following steps:

1. In the address field of your browser, type `https://` followed by the IP address of the virtual appliance, and then press **Enter**.

2. The admin login page opens. Type **admin** and **lan411cope** (both are case sensitive), and then click **Login**. Go to step 5.

3. The Welcome page opens. Click **Continue**

The Management Network Interface page opens.
6. Review the settings you previously entered, and then click Next. The Password Management page opens.

7. In the appropriate fields, type your new admin password, and then click Next. The Host Name and Domain page opens.
8. In the appropriate fields, type the host name and the network domain name, and then click **Next**. The DNS Settings page opens.

9. Click the + button, and then type the IP address of the DNS server. Click **Next**. The NTP Settings page opens.

**Note:** Please set the first NTP server to be pool.ntp.org. This will allow the Stealthwatch appliance to access the random ntp.org pool of NTP servers to set the appliance’s time.
10. You can accept the default setting or enter another server by entering the IP address of your NTP server or selecting a name by clicking the list icon and selecting one from the drop-down list. See Configuration through the Appliance Admin Interface.

12. Review your settings, and then click **Apply**. The confirmation dialogue opens.

13. Allow a few minutes for your new system settings to take effect and then click **Next**. When finished, the login page for the appliance opens.

14. Enter the login credentials, and then click **Login**.

15. Do you have any other appliances to configure?
   - If yes, return to Step 1 and repeat this procedure for the next appliance. Remember to configure the primary SMC last.
   - If no, go to the next step.

Expand Data Storage and Resource Allocations

To install a virtual appliance, you may need to expand the available data storage. Also, you may want to expand the appliance resource allocations to improve performance.

- For data storage ranges and resource allocation information, see the Resource Requirements: Data Storage section.
- If you increase the virtual machine memory using another method on your Hypervisor host, restart the appliance after you have saved your changes.

To expand the virtual appliance data storage, complete the following steps:

1. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Power off the virtual machine.
4. Access the virtual machine console.
5. Click on the page, and then do the following:
   - a. Type **sysadmin**, and then press **Enter**.
   - b. When the password prompt appears, type **lan1cope**, and then press **Enter**.

The System Configuration menu opens.
6. Select the **Advanced** option, and then press **Enter**. The Advanced menu page opens.

7. Select the **DataStorageExpansion** option. The Data Storage Expansion page opens.
8. Review the information and change it as needed. To save your changes, select \textbf{Yes}, and press \textbf{Enter}. The Warning page opens.

![Warning Page]

9. Select \textbf{Yes}, and then press \textbf{Enter}. The virtual appliance restarts and implements the changes.

10. Press \textbf{Ctrl+Alt} to exit the console environment.

11. Confirm the changes made to the data storage.

**Configuration through the Appliance Admin Interface**

This section provides the following procedures to complete the configuration of a virtual appliance using its Appliance Admin interface:

1. \textbf{Log in to the Appliance Administration Interface}
2. \textbf{Configuring a Virtual Appliance}
3. \textbf{Restart the Virtual Appliance}

**Log in to the Appliance Administration Interface**

To log in to the Appliance Administration (Admin) interface, complete the following steps:

**Notes:**

- The supported browsers for Stealthwatch are Internet Explorer version 11 and later, and the latest versions of Firefox, Google Chrome, and Safari.
- If you have trouble loading any of the pages, try a different browser, or clear your browser cache, close and re-open your browser, and then log in again.
1. In the address field of your browser, type https:// followed by the IP address of the virtual appliance, and then press Enter.

   **Note:** Depending on the speed of your VM host, it may take approximately 30 minutes for all services to boot up.


3. In the **User Name** field, type **admin**.
4. In the **Password** field, type the admin password you created in the appliance setup.
5. Click **Login**. The Appliance Admin interface Home page opens.

6. Continue with the next section, “Configure the Advanced Settings.”

**Configure the Advanced Settings**

If you want the Flow Sensor VE to identify applications, configure the following settings for your Flow Sensor VE:

1. In the Web Client Admin Appliance, select **Configuration > Advanced Settings**.
2. Select the **Export Application Identification** check box. By default, this option is not selected.
3. In the Cache Mode section, select one of the following options based on your method for monitoring flows:
   - The **Use single, shared, cache for all monitoring ports** option is typically used for systems that monitor flows using the TAP method.

© 2018 Cisco Systems, Inc. All Rights Reserved.
- The **Use independent caches for each monitoring port** option is typically used to experience better performance and for systems that monitor flows using the SPAN method.

**Restart the Virtual Appliance**

To restart the virtual appliance, complete the following steps:

1. On the Appliance Admin interface menu, select **Operations > Restart Appliance**.

   ![Restart Appliance Menu](image)

   The confirmation dialog opens.

   ![Confirmation Dialog](image)

   2. Click **Yes**.

   3. After you restart the appliance, continue installing and configuring your appliances in the order shown in **Configuring the Individual Appliances**. After you activate the product licenses on the appliance, the Flow Sensor VE will begin collecting data from the VM environment and sending it to the NetFlow collector. See the **Downloading and Licensing Guide** for details.

   Congratulations, you have now completely installed and configured the Flow Sensor VE!
- **SMC Client Enterprise Tree**: The Flow Sensor will be listed on the SMC Client Enterprise tree under the **Flow Sensors** and **VM Servers** branches.

- **Traffic Detection**: The Flow Sensor will appear on the SMC Enterprise tree when the Flow Sensor has an active license, detects traffic, and sends data to the Flow Collector, which sends data to the SMC.

- Please see the *SMC Client Online Help* and the *Downloading and Licensing Guide* for more information.