Stealthwatch® System

Hardware Installation Guide

(for Stealthwatch System v6.9.1)
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placing the Flow Sensor Inside Your Firewall</td>
<td>19</td>
</tr>
<tr>
<td>SPAN Ports</td>
<td>20</td>
</tr>
<tr>
<td><strong>Installation</strong></td>
<td>23</td>
</tr>
<tr>
<td>Overview</td>
<td>23</td>
</tr>
<tr>
<td>Mounting the Appliance</td>
<td>23</td>
</tr>
<tr>
<td>Hardware Included with the Appliance</td>
<td>23</td>
</tr>
<tr>
<td>Additional Required Hardware</td>
<td>24</td>
</tr>
<tr>
<td>Changing the Default User Password</td>
<td>26</td>
</tr>
<tr>
<td>Connecting to the Appliance</td>
<td>26</td>
</tr>
<tr>
<td>Changing the Default IP Addresses</td>
<td>27</td>
</tr>
<tr>
<td>Change the sysadmin User Password</td>
<td>31</td>
</tr>
<tr>
<td>Change the root User Password</td>
<td>33</td>
</tr>
<tr>
<td>Connecting the Appliance to the Network</td>
<td>36</td>
</tr>
<tr>
<td>Types of Servers</td>
<td>36</td>
</tr>
<tr>
<td>Connecting to the Network</td>
<td>45</td>
</tr>
</tbody>
</table>
INTRODUCTION

Overview

This guide explains how to install Stealthwatch System hardware products. It describes the Stealthwatch System components and how they are placed in the system, including the integration of the Flow Sensors. Also, this guide describes the mounting and installation of the Stealthwatch System hardware.

This chapter includes the following topics:

- Audience
- How to Use This Guide
- Common Abbreviations
- Introduction

Audience

This guide is designed for the person responsible for installing Stealthwatch system hardware. We assume that you already have some general understanding of installing network equipment (Flow Sensor, Flow Collector, UDP Director, and the Stealthwatch Management Console).

For information on configuring Stealthwatch System products, please refer to the Stealthwatch System Hardware Configuration Guide.

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>2 - Pre-Configuration Considerations</td>
<td>Describes the Stealthwatch system components and their placement and the configuration of the firewall for communications</td>
</tr>
<tr>
<td>3 - Installation</td>
<td>Describes the mounting and installation of Stealthwatch hardware</td>
</tr>
</tbody>
</table>
The following abbreviations appear in this guide:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone (a perimeter network)</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server/Service</td>
</tr>
<tr>
<td>FC</td>
<td>Flow Collector</td>
</tr>
<tr>
<td>FS</td>
<td>Flow Sensor</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol (Secure)</td>
</tr>
<tr>
<td>ISE</td>
<td>Identity Services Engine</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PCIe</td>
<td>Peripheral Component Interconnect Express</td>
</tr>
<tr>
<td>SMC</td>
<td>Stealthwatch Management Console</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SPAN</td>
<td>Switch Port Analyzer</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>TAP</td>
<td>Test Access Port</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
</tbody>
</table>
PRE-CONFIGURATION CONSIDERATIONS

Overview

This chapter examines the considerations you should make before installing and configuring your Stealthwatch appliances. It explains where to place Stealthwatch system products and how to integrate them into your network.

This chapter includes the following topics:

- CIMC Default Password
- Stealthwatch Components
- Placement Considerations
- Configuring Your Firewall for Communications
- Integrating the Flow Sensor into Your Network

CIMC Default Password

The Cisco Integrated Management Controller (CIMC) enables access to the server configuration and a virtual server console, as well as monitors for hardware health. Use the following default password to log in to the CIMC: Admin123.

WARNING! Once you log in, change the default password to protect the security of your network.

Stealthwatch Components

The Stealthwatch system is made up of several hardware components that gather, analyze, and present information about your network to improve network performance and security.
This section describes the major Stealthwatch components.

**Stealthwatch Management Console**

The Stealthwatch Management Console (SMC) is the control center for Stealthwatch. It manages, coordinates, configures, and organizes all of the different components of the system. The SMC client software allows you to access the SMC’s user-friendly graphical user interface (GUI) from any local computer with access to a Web browser. With the SMC you can easily access real-time security and network information about critical segments throughout your enterprise.

Featuring Java-based platform independence, the SMC enables:

- Centralized management, configuration, and reporting for up to 25 Stealthwatch Flow Collectors
- Graphical charts for visualizing traffic
- Drill-down analysis for troubleshooting
- Consolidated and customizable reports
- Trend analysis
- Performance monitoring
- Immediate notification of security breaches

**Flow Collector**


The Flow Collector aggregates high-speed network behavior data from multiple networks or network segments to deliver end-to-end protection and improve performance across geographically dispersed networks.

As the Flow Collector receives data, it identifies known or unknown attacks, internal misuse, or misconfigured network devices, regardless of packet encryption or fragmentation. Once Stealthwatch identifies the behavior, the system can take any action you have configured it to take, if any, for that kind of behavior.

**Flow Sensors**

The Stealthwatch Flow Sensor is a network appliance that operates similarly to a traditional packet capture appliance or IDS in that it plugs into a switch port analyzer (SPAN), mirror port, or Ethernet test access port (TAP). The Flow Sensor augments visibility into the following network areas:

- Where NetFlow is not available.
- Where NetFlow is available, but you want deeper visibility into performance metrics and packet data.
By directing the Flow Sensor 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 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.

**UDP Director**

The Stealthwatch UDP Director is a high-speed, high-performance UDP packet replicator. The UDP Director is very helpful in redistributing NetFlow, sFlow, syslog, or Simple Network Management Protocol (SNMP) traps to various collectors. It can receive data from any connectionless UDP application and then retransmit it to multiple destinations, duplicating the data if required.

**Note:** When you use the UDP Director High Availability (HA) configuration (failover), you must connect two UDP Director appliances with crossover cables. For specific instructions, see “Connecting to the Network” on page 45.*

**Placement Considerations**

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.
Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

**Note:** When you place a Flow Collector outside a firewall, we recommend that you turn off the setting “Accept traffic from any exporter.”
Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor 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.

The Flow Sensor 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)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

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 diagram and tables shown in this section to configure your network so that the appliances can communicate through the network.

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>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>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>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>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>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>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 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** are ones that may be used according to your own network needs.
Integrating the Flow Sensor into Your Network

The Stealthwatch Flow Sensor is versatile enough to integrate with a wide variety of network topologies, technologies, and components. While not all network configurations can be discussed here, the examples may help you determine the best setup for your monitoring needs.

Before you install a Flow Sensor, you must make several decisions about your network and how you want to monitor it. Be sure to analyze both your network's topology and your specific monitoring needs. It is recommended that you 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.
The following sections explain how to integrate a Stealthwatch Flow Sensor appliance into your network using the following Ethernet network devices:

- TAPs
- SPAN Ports

**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.

This section explains the following ways to use TAPs:

- Using Electrical TAPs
- Using Optical TAPs
- Using TAPs Outside Your Firewall
- Placing the Flow Sensor Inside Your Firewall

**Note:** In a network using TAPs, the Flow Sensor 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 is connected to a unidirectional TAP that is capturing only one direction of traffic on each port, then the Flow Sensor will not capture performance monitoring data.

**Using Electrical TAPs**

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

Note: If the connection between the monitored networks is an optical connection, then the Stealthwatch Flow Sensor 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 monitor traffic between your firewall and other networks, connect the Stealthwatch management port to a switch or port outside of the firewall.

WARNING! We strongly recommend 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.
Placing the Flow Sensor Inside Your Firewall

To monitor traffic between internal networks and a firewall, the Flow Sensor 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 Monitor Port 1 is connected to the mirror port, as shown in the following illustration:

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.
An optical splitter configuration is shown below.

**SPAN Ports**

You can also connect the Flow Sensor to a switch. However, because a switch does not repeat all traffic on each port, the Flow Sensor 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 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 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 can monitor all traffic to, from, and within the network of interest, as well as other networks.

**Note:** In all cases, we recommend 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.
INSTALLATION

Overview

This chapter includes the procedures for installing the Stealthwatch hardware into your environment.

This chapter includes the following topics:

- Mounting the Appliance
- Changing the Default User Passwords
- Connecting the Appliance to the Network

Mounting the Appliance

You can mount Stealthwatch products directly in a standard 19" rack or cabinet. You can also install them in any other suitable cabinet or on a flat surface.

**Note:** When mounting an appliance in a rack or cabinet, follow the instructions included in the rail mounting kits.

When determining where to place an appliance, make sure that clearance to the front and rear panels is as follows:

- The front-panel indicators can be read easily
- Access to ports on rear panel is sufficient for unrestricted cabling
- The rear panel power inlet is within reach of a conditioned AC power source.
- Airflow around the appliance and through the vents is unrestricted.

Hardware Included with the Appliance

The following hardware is included with Stealthwatch System products:

- AC power cord
- Access keys (for front face plate)
Rail kit for rack mounting or mounting ears for smaller appliances
For the Flow Collector 5000 series appliances, a 10 GB SFP cable

Additional Required Hardware

You must provide the following additional required hardware:

- Mounting screw for a standard 19" rack
- Uninterruptible power supply (UPS) for each Stealthwatch System product you are installing.
- Ethernet cables as shown in the following table, based on the product you are installing and the configuration you ordered. You can use the Total columns as a checklist to help you plan for the quantity you need.

<table>
<thead>
<tr>
<th>Product</th>
<th>Management Ports</th>
<th>Monitoring Port(s)</th>
<th>Total Copper</th>
<th>Total Fiber-Optic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMC 1000/1010</td>
<td>1 Copper</td>
<td>Not Used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMC 2000/2010</td>
<td>1 Copper</td>
<td>Not Used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMC 2200</td>
<td>2 Copper</td>
<td>Not Used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 1000/1010</td>
<td>1 Copper</td>
<td>1 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 2000/2010</td>
<td>1 Copper</td>
<td>Up to 3 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 4000/4010</td>
<td>1 Copper</td>
<td>Up to 3 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 4200</td>
<td>2 Copper</td>
<td>1 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 5000 engine</td>
<td>2 Copper</td>
<td></td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>FC 5000 database</td>
<td>2 Copper</td>
<td></td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>FC 5020 engine</td>
<td>1 Copper</td>
<td>1 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 5020 database</td>
<td>1 Copper</td>
<td>1 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 5200 engine</td>
<td>1 Copper</td>
<td>1 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC 5200 database</td>
<td>1 Copper</td>
<td>1 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Management Ports</td>
<td>Monitoring Port(s)</td>
<td>Total Copper</td>
<td>Total Fiber-Optic</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>FS 250</td>
<td>1 Copper</td>
<td>Up to 2 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS 1000/1010</td>
<td>1 Copper</td>
<td>Up to 3 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS 1200</td>
<td>2 Copper</td>
<td>Up to 5 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS 2000/2010</td>
<td>1 Copper</td>
<td>Up to 5 Copper</td>
<td>OR</td>
<td>Up to 3 Copper and Up to 2 Base-SX LC</td>
</tr>
<tr>
<td>FS 2200</td>
<td>2 Copper</td>
<td>Up to 5 Copper</td>
<td></td>
<td>Up to 2 Fiber-Optic</td>
</tr>
<tr>
<td>FS 3000/3010</td>
<td>1 Copper</td>
<td>Up to 2 Fiber optic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS 3200</td>
<td>2 Copper</td>
<td>Up to 2 SFP-10G-SR-S 10GBASE-SR SFP Module, Enterprise-Class</td>
<td>OR</td>
<td>SFP-10G-LR-S 10GBASE-LR SFP Module, Enterprise-Class</td>
</tr>
<tr>
<td>FS 4200</td>
<td>2 Copper</td>
<td>Up to 2 10 GB SFP+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP 2000/2010</td>
<td>1 Copper</td>
<td>Up to 3 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP 2200</td>
<td>2 Copper</td>
<td>Up to 5 Copper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC 1020</td>
<td>1 Copper</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Ethernet Cables Needed**

- To configure locally (optional), use one of the following methods:
  - Laptop with a video cable and a USB cable (for the keyboard)
  - Video monitor with a video cable and keyboard with a USB cable
Changing the Default User Passwords

This section describes how to connect to the appliance and then change the default user passwords.

Connecting to the Appliance

You can connect to the appliance in one of two ways:

- with a keyboard and monitor
- with a laptop (and a terminal emulator)

**Note:** For new products, SSH is disabled. You must log into the appliance Administration Web interface to enable it.

Connecting with a Keyboard and a Monitor

To configure the IP address locally, complete the following steps:

1. Plug in the power cable to the appliance.
2. Push the Power button to turn on the appliance and wait for it to finish booting up completely. Do not interrupt the boot up process.

**Note:**
- The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.
- Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

3. Connect the keyboard:
   - If you have a standard keyboard, connect it to the standard keyboard connector.
   - If you have a USB keyboard, connect it to a USB connector.

4. Connect the video cable to the video connector. The login prompt appears.
5. Continue with the section, “Changing the Default IP Addresses” on page 27.

Connecting with a Laptop

You can also connect to the appliance with a laptop, which must have a terminal emulator.

To connect to an appliance with a laptop, complete these steps:

1. Connect your laptop to the appliance using one of the following methods:
- Connect an RS232 cable from the serial port connector (DB9) on your laptop to the Console Port on the appliance.
- Connect a crossover cable from the Ethernet port on your laptop to the Management port on the appliance.

2. Boot up your laptop.
3. Connect power to the appliance. Press the Power button to turn on the appliance.

**Note:**
- The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.
- Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

4. On the laptop, make a connection into the appliance.

**Note:** You can use any available terminal emulator to communicate with the appliance.

5. Apply the following the settings:
   - BPS: 9600
   - Data bits: 8
   - Stop bit: 1
   - Parity: None
   - Flow Control: None

The login screen and login prompt are displayed.

6. Continue with the next section, Changing the Default IP Addresses

### Changing the Default IP Addresses

Once you have connected to the appliance, you need to configure the IP addresses. The appliances already have default IP addresses, but you should configure them to suit your network.

1. Log in to the System Configuration program by doing the following:
   - Type `sysadmin`, and then press **Enter**.
   - When the password prompt appears, type `lan1cope`, and then press **Enter**.
   - At the next prompt, type `SystemConfig`, and then press **Enter**.

The System Configuration menu opens.
2. Select **Management**, and then press **Enter**. The IP Address page opens.

3. Do the following:
   - Type a new IP address based on your environment.
   - Select **OK**, and then press **Enter** to continue.
     The IP netmask page opens with the default value.
4. Do the following:
   - Accept the default value or enter a new IP Netmask address based on your environment.
   - Select **OK**, and then press **Enter** to continue.

   The Broadcast Address page opens.

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

   The Gateway Address page opens with the default gateway server IP address.
6. Do the following:

- Accept the default value or enter a new one based on your environment.
- Select OK, and then press Enter to continue.

The confirmation page opens.

7. Review the information. Are the settings correct?

- If yes, select Yes, and then press Enter to continue. The system restarts and implements the changes. On completion, the Login page opens.
8. If no, select No to make corrections. The IP Address page opens so that you can enter your changes. After the changes are made and you accept the settings, the Restart page opens. Press Enter to implement your changes.

Change the sysadmin User Password

To ensure that your network is secure, you must change the default sysadmin password for appliances.

**Note:** Be sure that you have logged in as sysadmin to begin this procedure.

To change the sysadmin password, complete the following steps:

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

   ![System Configuration Menu]

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

   The prompt for a new password appears.

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

   **Note:** The password must be between 5 and 30 alphanumeric characters in length with no spaces. You also may use the following special characters: $.-!@#%_=?;{}()

4. Type the password again, and then press **Enter**.
5. When your password is accepted, press **Enter** again to return to the System Configuration menu.

6. Continue with the next section, “Change the root User Password.”

**Change the root User Password**

After you change the default sysadmin user password, you must change the default root user password to protect the security of your network further.

To change the root user password, complete the following steps:

1. Now in following steps you can change the password for the root login. First you need to go to the root shell.

2. On the System Configuration menu, select **Advanced**, and then press **Enter**. The Advanced menu appears.
3. Select **RootShell**, and then press **Enter**. A prompt for the root password appears.

4. Type the current root password, and then press **Enter**. The root shell prompt appears.

5. Type **SystemConfig**, and then press **Enter**. This returns you to the System Configuration menu so that you can change the root password.

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

8. Retype the new root password, and then press **Enter**.
9. When your password change is successful, press **Enter**. You have now changed both of your default sysadmin and root passwords. This returns you to the System Configuration Console menu.
10. Select **Cancel** and press **Enter**. The System Configuration Console closes and the root shell prompt appears.

11. Type **exit** and press **Enter**. The login prompt appears.

12. Press **Ctrl+Alt** to exit the Console environment.

13. Continue with the next section, “Connecting the Appliance to the Network.”

## Connecting the Appliance to the Network

The procedure to connect each appliance to the network is the same. The only difference for connection is type of appliance you have.

To connect your appliance to the network, complete the following steps:

1. Select your appliance from the types of servers shown below.
2. Follow the procedure for connecting the appliance to the network in the section, “Connecting to the Network” on page 45.

### Types of Servers

This section illustrates the types of Stealthwatch appliances used in a network.

**Note:** The Cisco servers (the “200” series, such as 2200 or 4200) use the same server, UCSC-C220-M4S, except for the Flow Collector 5200, which uses UCSC-C240-M4S2 (2RU). The variations in appliances are in NIC cards, processor, memory, storage and RAID. For further information about each appliance, see its specification sheet in the Documentation Library or the Lancope Community web site (community.lancope.com) The images shown here indicates the NIC ports used.
SMCs 1000 & 2000 and Flow Collectors 1000 & 2000

This appliance is used for the SMCs 500/1000, 1000 and 2000, the Flow Collectors 1000 and 2000, and the Flow Sensors 2000 and 3000.

Height: 1.68 inches (4.3 cm)
Width: 18.99 inches (48.24 cm) with rack latches
17.08 (43.4 cm) without rack latches
Depth: 27.8 inches (70.67 cm) with power supplies and bezel
28.6 inches (72.53 cm) without power supplies and bezel

Heat Dissipation: 2,891 BTUs per hour maximum
Power: Redundant, hot swappable: 750W, 50/60 Hz; Auto Ranging (100V to 240V)

SMC 1010, Flow Collectors 1010 & 4010, Flow Sensors 2010, 3010, 4010 and UDP Director 2010

This appliance is used for the following models:

- SMC 1010
- Flow Collector 1010, Flow Collector 4010
- UDP Director 2010

Height: 1.68 inches (4.3 cm)
Width: 17.09 inches (43.4 cm)
Depth: 29.25 inches (74.3 cm)

Heat Dissipation: 2,891 BTUs per hour
Power: Redundant: 750W
SMC 2010 and Flow Collector 2010

This appliance is used for the SMC 2010 and the Flow Collector 2010.

Height: 1.68 inches (4.3 cm)  
Width: 17.09 inches (43.4 cm)  
Depth: 29.25 inches (74.3 cm)  
Heat Dissipation: 2,891 BTUs per hour  
Power: Redundant: 750W

SMC 2200

This server is used for the SMC 2200.

1. Reserved ports: 2; fiber - 10 GB SFP+  
2. CIMC management port: 1; 100/1000 copper  
3. Stealthwatch management port: 1; 100/1000 copper

Height: 1.7 inches (4.3 cm)  
Width: 16.9 inches (42.9 cm)  
Depth: 29.8 inches (75.8 cm)  
Heat Dissipation: 1741.13 BTU per hour maximum (estimated)  
Power: 2 redundant hot-swappable 750W; Auto Ranging (100V ~ 240V)

Flow Collector 4000

This appliance is used for the Flow Collector 4000.
Flow Collector 4200

This appliance is used for the Flow Collector 4200

- 1. Reserved ports: 2; 10 GB SFP+
- 2. CIMC management port
- 3. Stealthwatch management port: 1; 10/100/1000 copper
- 4. Monitoring port: 1; 100/1000 copper

Flow Collector 5000 Engine

Because the Flow Collector 5000 for NetFlow platform consists of two connected servers, the installation differs from other appliances. They are directly connected by a 10G SFP cable so that they function as a single appliance.

Use the supplied 10 GB SFP cable to connect these units at the port labeled eth2. Place these servers adjacent, vertically, to each other in the rack in order for the 10 GB SFP cable to reach. Each server uses a 1 GB copper Ethernet port to be used as a Management Port. Each server also has a dedicated iDRAC Enterprise port. Two onboard ports that are not used. These should have a port cover installed to discourage their use.

The image below shows the connection between the servers. The Flow Collector 5000 engine is above and the Flow Collector 5000 database is below.
Flow Collector 5000 Database.

This appliance is used for the Flow Collector 5000 database, which is paired with the Flow Collector 5000 engine.

Flow Collector 5020 and 5200 Engines

Because the Flow Collector 5020 for NetFlow platform and Flow Collector 5200 for NetFlow platform consist of two connected servers, the installation differs from other appliances. The servers are directly connected by a 10G SFP+ DA Cross Connect cable so that they function as a single appliance. Both of these Flow Collectors use the same Cisco server and appliance setup.

Note: Each of the engines for the Flow Collector 5020 and Flow Collector 5200 is paired with its matching database. Both of these engines use the same Cisco server and appliance setup. The following appliance is used for each of these two engines.

1. 10 GB SFP+ DA Cross Connect
2. CIMC management port
3. Stealthwatch management port: 1; 10/100/1000 copper
4. Monitoring port: 1; 10/100/1000 copper

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Height:</strong></td>
<td>1.7 inches (4.3 cm)</td>
</tr>
<tr>
<td><strong>Width:</strong></td>
<td>16.9 inches (42.9 cm)</td>
</tr>
<tr>
<td><strong>Depth:</strong></td>
<td>29.8 inches (75.8 cm)</td>
</tr>
</tbody>
</table>

**Heat Dissipation:** 1816.63 BTU per maximum hour (estimated)

**Power:** Redundant 770W;
AC input voltage: Nominal range 100-127 VAC, 200-240 VAC;
AC input frequency: Nominal range 50 to 60 Hz;
Max AC input current: 9.5 A at 100 VAC, 4.5 A at 208 VAC

**Flow Collector 5020 and 5200 Databases**

This appliance is used for the Flow Collector 5020 database and Flow Collector 5200 database, each of which is paired with its matching engine. Both of these database nodes use the same Cisco server and appliance setup. The following appliance is used for each of these two databases.

1. 10 GB SFP+ DA Cross Connect
2. CIMC management port
3. Stealthwatch management port

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Height:</strong></td>
<td>3.42 inches (8.67 cm)</td>
</tr>
<tr>
<td><strong>Width:</strong></td>
<td>18.96 inches (44.8 cm) with rack latches; 17.65 in. (44.8 cm) without rack latches</td>
</tr>
<tr>
<td><strong>Depth:</strong></td>
<td>30.18 inches (76.6 cm) with handles; 29.0 in. (73.8 cm) without handles</td>
</tr>
</tbody>
</table>

**Heat Dissipation:** 2492.78 BTU per hour maximum (estimated)

**Power:** Redundant 770W;
AC input voltage: Nominal range 100-127 VAC, 200-240 VAC;
AC input frequency: Nominal range 50 to 60 Hz;
Max AC input current: 11 A at 100 VAC, 7 A at 208 VAC
Flow Sensor 1000 and UDP Director (also known as FlowReplicator) 1000

This appliance is used for the Flow Sensor 1000 and the UDP Director 1000.

<table>
<thead>
<tr>
<th>Height: 1.67 inches (4.2 cm)</th>
<th>Heat Dissipation: 1039 BTUs per hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width: 17.09 inches (43.4 cm)</td>
<td>Power: Single: 250W</td>
</tr>
<tr>
<td>Depth: 15.5 inches (39.4 cm)</td>
<td></td>
</tr>
</tbody>
</table>

Flow Sensor 1010 and UDP Director 1010

This appliance is used for the Flow Sensor 1010 and the UDP Director 1010.

<table>
<thead>
<tr>
<th>Height: 1.67 inches (4.2 cm)</th>
<th>Heat Dissipation: 1040 BTUs per hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width: 17.09 inches (43.4 cm)</td>
<td>Power: Single: 250W</td>
</tr>
<tr>
<td>Depth: 15.5 inches (39.4 cm)</td>
<td></td>
</tr>
</tbody>
</table>

Flow Sensor 1200

This server is used for the Flow Sensor 1200.

1. Monitoring ports: 5; 100/1000 copper
2. CIMC management port: 1; 100/1000 copper
3. Stealthwatch management port: 1; 100/1000 copper

| Height: 1.7 inches (4.3 cm) | Heat Dissipation: 664.86 BTU per hour maximum (estimated) |
| Width: 16.9 inches (42.9 cm) | Power: 2 redundant hot-swappable 750W; Auto Ranging (100V ~ 240V) |
| Depth: 29.8 inches (75.8 cm) |

**Flow Sensor 2200**

This server is used for the Flow Sensor 2200.

1. Monitoring ports: 5; 100/1000 copper
2. Monitoring ports: 2; 1 GB Base-SX LC

**Note:** You can use either copper cable or the fiber optic cable, but not both

3. CIMC management port: 1; 100/1000 copper
4. Stealthwatch management port: 1; 100/1000 copper

| Height: 1.7 inches (4.3 cm) | Heat Dissipation: 1164.77 BTU per hour maximum (estimated) |
| Width: 16.9 inches (42.9 cm) | Power: 2 redundant hot-swappable 750W; Auto Ranging (100V ~ 240V) |
| Depth: 29.8 inches (75.8 cm) |

**Flow Sensor 3200**

This server is used for the Flow Sensor 3200

1. Monitoring ports: 2; SFP-10G-SR-S 10GBASE-SR SFP Module, Enterprise-Class or SFP-10G-LR-S 10GBASE-LR SFP Module, Enterprise-Class
2. CIMC management port: 1; 100/1000 copper
3. Stealthwatch management port: 1; 100/1000 copper
Flow Sensor 4000

The same appliance for the Flow Sensor 2000 and Flow Sensor 3000 is used for the Flow Sensor 4000. However, this Flow Sensor supports only 10 GB interfaces and has four monitor ports.

Height: 1.68 inches (4.26 cm)
Width: 18.99 inches (48.24 cm) with rack latches
16.69 (42.4 cm) without rack latches
Depth: 30.39 inches (77.2 cm) with power supplies and bezel
29.02 (73.73 cm) without power supplies and bezel

Heat Dissipation: 2446.5 BTUs per hour maximum
Power: Redundant, hot swappable; 717W

Flow Sensor 4200

This server is used for the Flow Sensor 4200.

1. Monitoring ports: 4; 10 GB SFP+
2. CIMC management port: 1; 100/1000 copper
3. Stealthwatch management port: 1; 100/1000 copper

Height: 1.7 inches (4.3 cm)
Width: 16.9 inches (42.9 cm)
Depth: 29.8 inches (75.8 cm)

Heat Dissipation: 1282.64 BTU per hour maximum (estimated)
Power: 2 redundant hot-swappable 750W; Auto Ranging (100V ~ 240V)

UDP Director 2000, Flow Sensors 2000 and 3000

This appliance is the same as the previous one, but it also has two optional fiber optics ports. It is used for the Flow Sensor 2000, the Flow Sensor 3000, and the UDP Director (also known as FlowReplicator) 2000:
**Height:** 1.68 inches (4.26 cm)  
**Width:** 18.99 inches (48.24 cm) with rack latches  
17.08 (43.4 cm) without rack latches  
**Depth:** 27.8 inches (70.67 cm) with power supplies and bezel  
28.6 (72.53 cm) without power supplies and bezel

| **Heat Dissipation:** | 2,891 BTUs per hour maximum  
**Power:** | 750 W AC, 50/60 Hz; Auto Ranging (100V to 240V) |

**UDP Director 2200**

This server is used for the UDP Director 2200.

1. Monitoring ports: 3; 100/1000 copper  
2. Reserved ports: 2; 1 GB Base-SX LC

Note: You can use either copper cable or the fiber optic cable, but not both

3. CIMC management port: 1; 100/1000 copper  
4. Stealthwatch management port: 1; 100/1000 copper  
5. HA Cross Connect ports: 2

| **Height:** | 1.7 inches (4.3 cm)  
**Width:** | 16.9 inches (42.9 cm)  
**Depth:** | 29.8 inches (75.8 cm) |

| **Heat Dissipation:** | 1164.77 BTU per hour maximum (estimated)  
**Power:** | 2 redundant hot-swappable  
750W; Auto Ranging (100V ~ 240V) |

**Connecting to the Network**

To connect the appliance to your network, complete the following steps:

1. Connect an Ethernet cable to the management port, located at the rear of the appliance.  
2. Connect at least one monitor port for Flow Sensors and UDP Directors. Refer to the hardware table on page 24 for the appropriate cable for your appliance.
Important: For the UDP Director HA, connect the two UDP Directors by crossover cables. Connect the eth2 port of one UDP Director to the eth2 port of the second UDP Director. Similarly, connect the eth3 port of each UDP Director with a second crossover cable. The cable can be fiber or copper.

Note: Be sure to note the Ethernet label (eth2, eth3, etc.) for each port. These labels correspond to the network interfaces (eth2, eth3, etc.) that are displayed on, and may be configured from, the Home page of the Appliance Admin interface.

3. Connect the other end of the Ethernet cables to your network’s switch.
4. Connect the power cords to the power supply. Some appliances have two power connections: Power Supply 1 and Power Supply 2.
5. Push the Power button to turn on the appliance.

Note:
- You may need to remove the front panel to apply power.
- The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.
- Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

6. To configure the appliance, see the *Stealthwatch System v6.9.0 Hardware Configuration Guide*. 