IPS-1 Sensor

R71

Administration Guide
More Information

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=10505

For additional technical information about Check Point visit Check Point Support Center
(http://supportcenter.checkpoint.com).

Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your
comments to us (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on IPS-1 Sensor R71
Administration Guide).

© 2010 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under
licensing restricting their use, copying, distribution, and decompilation. No part of this product or related
documentation may be reproduced in any form or by any means without prior written authorization of Check
Point. While every precaution has been taken in the preparation of this book, Check Point assumes no
responsibility for errors or omissions. This publication and features described herein are subject to change
without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph
(c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR
52.227-19.

TRADEMARKS:

Please refer to our Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Please refer to our Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a
list of relevant copyrights.
Chapter 1

Overview of IPS-1

IPS-1 is an intrusion prevention system (IPS) that delivers protection from a wide-range of network threats using an IPS-1 Sensor that can be placed either on the perimeter of your network or at any location in your internal network.

Some of the benefits of IPS-1 include:

- Unified security management
- Mission-critical protection against known and unknown attacks
- Granular forensic analysis
- Flexible deployment
- Confidence Indexing

In This Chapter

<table>
<thead>
<tr>
<th>IPS-1 Key Benefits</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS-1 System Architecture</td>
<td>5</td>
</tr>
<tr>
<td>IPS-1 Sensor Deployment</td>
<td>5</td>
</tr>
<tr>
<td>Managing IPS Profiles and Protections</td>
<td>6</td>
</tr>
</tbody>
</table>

IPS-1 Key Benefits

The IPS-1 Intrusion Prevention System provides accurate, high performance protection against known and unknown attacks. You can customize its features to suit your organization's particular needs. IPS-1 offers many benefits, including:

Unified Security Management

- Seamless integration into the Check Point security infrastructure
- Devices and policies are managed from the same console as all other Check Point security products
- Alerts and logs are configured and reviewed using the same tools as all other Check Point security products

Trusted Intrusion Prevention

- Smart intrusion detection
- Customizable intrusion prevention
- Customizable Confidence Indexing
- Customizable attack signatures
- Automatic attack signature updates

IPS Simplified

- Quick deployment
- Flexible deployment modes
- Minimal-impact design
- Centralized, scalable management
- Customizable desktop GUI with real-time information and management

**Dynamic Shielding**
- Presents network intelligence including OS and application information, CVE vulnerabilities, and impact and remediation details.
- Determines anomalous behavior, reduces false positives and recognizes and dynamically shields vulnerable hosts against inevitable attacks.

**IPS-1 System Architecture**

An IPS-1 deployment includes the following components:
- **IPS-1 Sensor**: A device that is used exclusively for detecting and preventing network attacks, and sends alerts to the Security Management Server. The sensor enforces “dedicated” IPS protections.
- **Security Management Server**: The central management server which contains the object database and security policies. Security policies and IPS profiles are configured on the Security Management Server and installed on the IPS-1 sensors.
- **Log Server**: Receives alert information from the Security Management Server. The Log server can be installed with the Security Management server or as a separate server.
- **SmartConsole**: Windows-based remote graphical user interface (GUI) to the Security Management server for managing IPS-1 sensors, IPS profiles and IPS protections. The SmartConsole includes a number of independent interlinked clients, primarily:
  - **SmartDashboard** for configuring protections and managing the entire IPS-1 system.
  - **SmartView Tracker** for viewing, tracking, and analyzing alerts.

**IPS-1 Sensor Deployment**

IPS-1 Sensors should be deployed at natural choke points according to network topology. Usually, sensors should be just within the network firewall. We do not recommend placing sensors outside the firewall because the sensor will not be protected by the firewall and unfiltered traffic will place a heavy load on the sensor.

Ideally, network cores should also be protected with sensors. In some cases, such as in a complex switching environment in a network core, sensors need to be used for intrusion detection in passive mode.

Sensors’ monitoring interfaces are layer-3 transparent and do not have IP addresses. Each sensor has a management interface that requires an IP address that is routable to and from the Security Management Server. For enhanced security, we recommend that the management server be on a separate, out-of-band network.

**Inline Intrusion Prevention**

For intrusion prevention, sensors should be connected inline, so that all of the traffic to be monitored flows through the IPS-1 Sensor. In this configuration, sensors can drop traffic containing attacks, according to defined and configurable confidence indexing.

Inline sensors’ behavior upon failure can be configured to either open, passing through all traffic; or closed, severing the traffic path.

Inline sensors can be set to Detect-Only, to avoid the possibility dropping false-positive traffic. This way you can track what the sensor would have done in prevention mode. You can fine-tune your prevention settings in Detect-only/Monitor-only mode, and later change to prevention mode.
Passive Intrusion Detection

The IPS-1 Sensor can be placed out of the path of network traffic, in which case it performs intrusion detection only.

For the sensor to monitor traffic, a monitoring interface of the sensor should be connected to one of the following:

- A hub's port
- A switch's SPAN (or 'mirror') port
- A network tap

A network tap has advantages over a switch's SPAN port. For example, the switch could prevent (or be unable to send) some traffic out of the SPAN port.

For information on configuring and connecting the switch or tap, see the switch's or tap's documentation.

Managing IPS Profiles and Protections

Manage the IPS profiles and protections using the IPS tab of the Check Point SmartDashboard.

- To install the Check Point SmartDashboard, see the R71 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=10327).
Chapter 2

Managing the IPS-1 Sensors

You can connect to the IPS-1 Sensor directly to do these tasks:

- Change the IPS-1 Sensor Mode and other settings
- Reboot the IPS-1 Sensor
- Network Interface information

IPS-1 Protections and Profiles can only be changed using the SmartDashboard client.

In This Chapter

- Connecting to the IPS-1 Sensor 7
- IPS-1 Sensor Modes 7
- IPS-1 Sensor Configuration 9
- Rebooting the IPS-1 Sensor 9

Connecting to the IPS-1 Sensor

You can run commands on the IPS-1 Sensor in one of three ways, depending on hardware configuration:

- A connected keyboard and monitor.
- A serial console (DTE to DTE), using terminal emulation software such as HyperTerminal (from Windows) or Minicom (from Unix/Linux systems).
  Connection parameters for Check Point IPS-1 appliances are: 9600bps, no parity, 1 stop bit (8N1).
- An SSH connection to the Sensor's management interface (if sshd is configured).

IPS-1 Sensor Modes

In most cases, IPS-1 Sensors should be placed inline, so that all of the traffic to be monitored flows through the IPS-1 Sensor. This enables intrusion prevention. In this configuration, sensors can drop traffic detected as an attack. In some cases, such as in a complex switching environment in a network core, sensors may need to be placed in passive mode, in which case they perform intrusion detection only.

Inline Sensors' behavior upon failure can be configured to either:

- Open: passes all traffic through
- Closed: breaks the connection between the two sides

Inline Sensors can be set to Detect Only to avoid the possibility of blocking valid traffic. You can track what the Sensor would have done in prevention mode. You can fine-tune your prevention settings in Detect Only and then change to another Inline mode to use the configuration to prevent identified attacks.

The IPS-1 Sensor has four modes:

- **IDS - Passive**: The IPS-1 Sensor is not placed in the path of traffic. Packets are processed for attack detection without any impact on the flow of network traffic.
- **IPS - Inline, Detect only**: Inline intrusion detection. Packets are forwarded through to the network before processing for attack detection. In fault conditions, all packets are allowed. Detect only mode is also useful for checking whether an IPS-mode Sensor is responsible for dropped traffic.
• **IPS - Inline, fail-open**: Inline intrusion prevention. Packets are processed for attack detection and are forwarded to the network only in accordance with protection settings. In fault conditions, all packets are allowed.

• **IPS - Inline, fail-closed**: Inline intrusion prevention. Packets are processed for attack detection and are forwarded to the network only in accordance with protection settings. In fault conditions, all packets are dropped.

⚠️ **Warning** - Changing the Working Mode may stop the flow of network traffic. Make sure that your network topology is correct for the IPS-1 Sensor Working Mode that you choose.

Fault conditions are:

- The Sensor has not completing booting and initializing
- The Sensor loses power, or other hardware failure (dependent on hardware bypass NIC)
- When the Sensor has crashed (dependent on hardware bypass NIC)

When an interface pair is in bypass mode, as a result of a failure, the bypass interfaces in most Sensor models will act as a crossover connection between the two systems on either side of the sensor. The four front-left copper interfaces on the new 200C/F and new 500C/F will act as a straight-through connection when in bypass mode. All other hardware bypass pairs act as crossover connections when they are in bypass mode.

### Changing the Sensor Mode (Software)

The IPS-1 Sensor mode is set during sensor installation.

**To change the sensor mode from the command line:**

1. Run: `cpconfig`
2. Enter 3 to change the IPS-1 Sensor Configuration.
3. Select **Network Settings**.
4. Select **Set operating mode**.
5. Press Enter to select the Operating Mode and set one of the modes.
6. If you set the sensor to an IPS mode, set the interfaces to for the inline pairs. On certain appliances the inline pairs are already defined and cannot be changed.
7. Select **Save**.
8. Select **Return to main menu**.
9. Select **Quit**.
10. Enter 4 to exit the configuration menu.
11. Run: `reboot`

**To change the sensor mode from the SmartDashboard:**

1. Open the properties of the IPS-1 Sensor.
2. In the General page, set one of the Working Modes.
3. Install the policy on the IPS-1 Sensor for the changes to take effect.

⚠️ **Note** - If policy installation fails when the IPS-1 Sensor is set to an IPS-Inline Working Mode, log into the sensor’s CLI and check that the interfaces are set to work as inline pairs.

### Changing the Sensor Mode (Hardware)

The IPS-1 Sensor 50 models is ordered and delivered as SKU "P" for "IPS Monitor-Only" and "IPS (inline fail-open)" modes, or SKU "D" for "IPS (inline, fail-closed)" and "IDS (passive)" modes. Switching between the two configurations requires two steps in addition to changing the sensor's operating mode in software: an internal hardware setting change and a BIOS change.
1. Change the position of the red hardware jumper switch on the system's motherboard near the Ethernet ports on the front of the chassis.
   - For passthrough modes (monitor-only and fail-open), the switch must be positioned to the rear of the unit, near pins 6 & 7.
   - For non-passthrough modes (fail-closed and passive), the switch must be positioned to the front of the unit, near pins 1 and 12.

2. Boot the Sensor.
3. Wait for the following message during the POST:
   
   TO ENTER SETUP BEFORE BOOT
   PRESS <CTRL-ALT-ESC> OR <DEL> KEY
   
   Press the <Del> key or press the <Ctrl>, <Alt>, and <Esc> keys to enter the system's BIOS Setup.

4. On the 'Integrated Peripherals' screen, "Onboard By-PASS Active" should be set to "[Enabled]" for passthrough modes, and "[Disabled]" for non-passthrough modes.

5. Exit the BIOS Setup and continue with the boot process.

Warranty note: Check Point will not void the warranty of units that have been opened for this purpose. A Check Point SE is not required to make the change, but Professional Services can be arranged if the customer elects not to make the changes themselves.

---

**IPS-1 Sensor Configuration**

You can use `cpconfig` to:

- Display the Certificate fingerprint
- Reset the Secure Internal Communication Activation Key
- View network interface information, including MAC address and link status

To do this:
1. Log into the IPS-1 Sensor.
2. Run: `cpconfig`
   - Press 1 to reset the Secure Internal Communication Activation Key.
   - Press 2 to display the Certificate fingerprint.
   - Press 3 to view network interface information. The press Enter to access the network settings and select Network information.

3. Navigate the menu options to make your changes.

You can use `sysconfig` to:

- Change the host name, domain name and DNS servers
- Set the time and date
- Change the management interface IP address

To do this:
1. Log into the IPS-1 Sensor.
2. Run: `sysconfig`
3. Navigate the menu options to make your changes.

These changes take effect immediately.

---

**Rebooting the IPS-1 Sensor**

To shutdown or reboot an IPS-1 Sensor from the command line, use SecurePlatform's `shutdown` or `reboot` command. The operating system is completely shut down, not just Sensor processes.

To restart the IPS-1 Sensor processes without rebooting the sensor:
1. Run: expert
2. Enter the expert mode password.
   The default password is the same as the original admin password.
3. Run: cpstop
4. Run: cpstart
This chapter discusses setting up Check Point pre-installed appliances. For open servers, see the *R71 Installation and Upgrade Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=10327).

For considerations for sensor location and network topology, see IPS-1 Sensor Deployment (on page 5).

In This Chapter

- IPS-1 Sensor Appliance Models
- Preparing the Sensor's Environment

### IPS-1 Sensor Appliance Models

#### IPS-1 Sensor 50C

![IPS-1 Sensor 50C from front](image)

- Front — Two 10/100Mbps copper Ethernet front-panel interfaces used in IPS (inline) mode as an IPS pair with bypass support, or in IDS (passive) mode as two monitoring interfaces
- Two 10/100/1000Mbps copper Ethernet front-panel interfaces, of which one is the management interface and the other can be used in IDS (passive) mode as an additional monitoring interface

#### IPS-1 Sensor 500C

![IPS-1 Sensor500C from front](image)

- Front — Eight 10/100/1000Mbps copper Ethernet front-panel interfaces used in IPS (inline) mode as IPS pairs with bypass support, or in IDS (passive) mode as monitoring interfaces

#### IPS-1 Sensor 200C

![IPS-1 Sensor 200C from rear](image)

- Back — Four 10/100/1000Mbps copper Ethernet back-panel interfaces, of which one is the management interface and the others can be used in IDS (passive) mode as additional monitoring interfaces
IPS-1 Sensor 500F

Figure 3-4   IPS-1 Sensor 500F from front

- Front — Four 10/100/1000Mbps copper Ethernet front-panel interfaces used in IPS (inline) mode as IPS pairs with bypass support, or in IDS (passive) mode as monitoring interfaces
- Four 1000Mbps Fiber front-panel interface with bypass support

Figure 3-5   IPS-1 Sensor 200C from rear

- Back — Four 10/100/1000Mbps copper Ethernet back-panel interfaces, of which one is the management interface and the others can be used in IDS (passive) mode as additional monitoring interfaces.

IPS-1 Sensor 1000C

Figure 3-6   IPS-1 Sensor 1000c from rear

- Eight 10/100/1000 copper Ethernet back-panel interfaces used in IPS (inline) mode as IPS pairs with bypass support, or in IDS (passive) mode as monitoring interfaces
- Two 10/100/1000 built-in copper Ethernet back-panel interfaces, of which one is the management interface and the other should remain unused.

IPS-1 Sensor 1000F

Note - The interface labels of the 1000F model are the same as the interface labels for the 1000C model.

- Eight Gigabit fiber Ethernet back-panel interfaces used in IPS (inline) mode as IPS pairs with bypass support, or in IDS (passive) mode as monitoring interfaces
- Two 10/100/1000 copper Ethernet back-panel interfaces, of which one is the management interface and the other should remain unused.

Preparing the Sensor's Environment

These IPS-1 Sensors require the following:

Table 3-1   IPS-1 Sensor Environmental Requirements

<table>
<thead>
<tr>
<th></th>
<th>50C</th>
<th>500C/F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis size</td>
<td>1 Rack Unit (RU), 19&quot;</td>
<td></td>
</tr>
<tr>
<td>Amps AC</td>
<td>6.0/3.0</td>
<td>6.7/3.4</td>
</tr>
<tr>
<td>Voltage Input Range</td>
<td>100-240</td>
<td>100-127/ 200-240</td>
</tr>
</tbody>
</table>
## Setting Up Sensor Appliance Network Connections

Connect the management interface to the management network. On the 50C, the management interface is on the front panel. On other models, it should be one of the two built-in interfaces on the rear panel.

For working in IDS (passive), any or all of the remaining interfaces can be used as monitoring ports.

For working in inline IPS mode, the inline pairs must conform to hardware configuration:

- For the 50C, the inline pair is marked on the front panel.
- For the 500 models, inline pairs are in vertical groupings.

<table>
<thead>
<tr>
<th></th>
<th>50C</th>
<th>500C/F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</td>
<td>0°C to +40°C</td>
<td>+10°C to +35°C</td>
</tr>
<tr>
<td>Non-Operating Temperature</td>
<td>-20°C to +80°C</td>
<td>-40°C to +70°C</td>
</tr>
<tr>
<td>Non-Operating Relative Humidity</td>
<td>10-90%, non-condensing @ 35°C</td>
<td>90%, non-condensing @35°C</td>
</tr>
<tr>
<td>Emissions</td>
<td>FCC Class A Device</td>
<td></td>
</tr>
</tbody>
</table>
Index

C
Changing the Sensor Mode (Hardware) • 8
Changing the Sensor Mode (Software) • 8
Connecting to the IPS-1 Sensor • 7

D
Dynamic Shielding • 5

I
Inline Intrusion Prevention • 5
IPS Simplified • 4
IPS-1 Key Benefits • 4
IPS-1 Sensor 1000C • 12
IPS-1 Sensor 1000F • 12
IPS-1 Sensor 500C • 11
IPS-1 Sensor 500F • 12
IPS-1 Sensor 50C • 11
IPS-1 Sensor Appliance Models • 11
IPS-1 Sensor Appliances • 11
IPS-1 Sensor Configuration • 9
IPS-1 Sensor Deployment • 5
IPS-1 Sensor Modes • 7
IPS-1 System Architecture • 5

M
Managing IPS Profiles and Protections • 6
Managing the IPS-1 Sensors • 7

O
Overview of IPS-1 • 4

P
Passive Intrusion Detection • 6
Preparing the Sensor's Environment • 12

R
Rebooting the IPS-1 Sensor • 9

S
Setting Up Sensor Appliance Network
  Connections • 13

T
Trusted Intrusion Prevention • 4

U
Unified Security Management • 4