How to Send Logs from a Locally Managed 600/1100 Appliance to a Security Management/Log Server
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Version of this Document
Download the latest version of this document

To learn more, visit the Check Point Support Center

Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How to Send Logs from a Locally Managed 600/1100 Appliance to a Security Management/Log Server.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09 August 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
How to Send Logs from a Locally Managed 600/1100 Appliance to a Security Management/Log Server

Objective

This document explains how to view the locally managed gateway logs in SmartView Tracker or SmartLog.

Supported Versions

- For 600/1100 - R75.20 (any HFA) Gaia Embedded package
- For 1100 only - R77.20 (any HFA) Gaia Embedded package

Note that the Security Management Server version must be the same version as the Security Gateway or higher.
Tested with R77 Security Management Server only.

Supported Operating Systems

- All

Supported Appliances

- Check Point 600 Appliance
- Check Point 1100 Appliance

Before You Start

Related Documents and Assumed Knowledge

- Users need to be familiar with initial configuration of the Security Management Server and the Security Gateway.

Impact on the Environment and Warnings

- N/A
Step 1: Configuring SmartDashboard

To configure the 600 or 1100 Security Gateway in SmartDashboard:

1. Log in to your SmartDashboard.
2. In Network Objects, right click Check Point > Check Point > Security Gateway/Management and select Classic Mode.
   The General Properties page opens.
3. Enter a Name for the gateway and an IP Address.
4. In Hardware, select 1100 Appliances and select the applicable Version and Type.
5. In Software Blades, make sure that only Firewall is selected.
6. Click Communication.
   The Trusted Communication window opens.
8. Enter the One-time password and confirm it.
9. Select Initiate trusted communication automatically when the Gateway connects to the Security Management server for the first time.
Step 2: Configuring the Locally Managed Appliance

To configure your 600 or 1100 appliance you must enter information in the Log Servers page including a SIC name and password. You can obtain the SIC name with GuiDBedit or with a CLI command.

To get the SIC name through GuiDBedit:
2. Open Table > Network Objects and locate the log server object.
3. Note the value in sic_name.

To get the SIC name through the CLI:
1. On the Security Management / Log Server run this CLI command:
   `$CPDIR/bin/cpprod_util CPPROD_GetValue SIC MySICname 0`
2. Note the value.

To configure the 600 / 1100 appliance:
1. Log in to the 600 / 1100 Appliance WebUI.
2. Select Logs & Monitoring > Log Servers.

10. Click OK twice.
11. From the menu button, select Policy > Install Database.
4. Enter the **Management Server IP address**, the **SIC Name**, and the **SIC password** (use the same SIC password that you entered in SmartDashboard and confirm it).

![SmartDashboard configuration](image)

5. **Click Apply.**

In SmartDashboard, a pop up message shows that trust was established.

![Trust established](image)

---

**Verifying**

1. **Make sure** Firewall logs from the Security Gateway are shown in SmartView Tracker or SmartLog (if enabled).

![SmartView Tracker](image)

2. **From the Security Management Server CLI** confirm that there is an established connection from the Security Gateway on port 257.

Run:

```
netstat -tupan
```