How to Troubleshoot Logging Issues

29 August 2011
© 2011 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:

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

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.
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 Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=12298
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 August 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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 Troubleshoot Logging Issues).
## Contents

**Important Information**.................................................................................................................. 3  
**How To Troubleshoot Logging Issues** ....................................................................................... 5  
  - Objective ............................................................................................................................................... 5  
  - Supported Operating Systems ............................................................................................................. 5  
  - Supported Appliances .......................................................................................................................... 5  
  - Supported Versions .............................................................................................................................. 5  
**Impact on the Environment and Warnings** .................................................................................. 5  
**Troubleshooting Procedures** ......................................................................................................... 5  
  - Preliminary Questions .......................................................................................................................... 5  
  - Incorrectly Configured Standalone Deployments ............................................................................... 6  
  - The Security Management server is not in the Listening State ....................................................... 6  
  - Network Connectivity ......................................................................................................................... 6  
  - Installing a Policy ............................................................................................................................... 7  
  - Making Sure that Logs are Sent ......................................................................................................... 7  
  - Verifying the Masters File .................................................................................................................. 7  
  - Using tcpdump to Verify Network Connections .............................................................................. 7  
  - Doing a Log Switch ............................................................................................................................ 8  
  - Removing Possible Corrupted Files .................................................................................................. 8  
  - Using Debug ......................................................................................................................................... 8  
**Verification** ........................................................................................................................................ 8  
**Index** .................................................................................................................................................. 9
How To Troubleshoot Logging Issues

Objective

Sometimes the Security Management server stops receiving logs from the Security Gateways that it manages. In this situation, the Security Gateways save their log files locally, using up disk space according to the quantity of log entries generated.

This document contains practical troubleshooting procedures that can be used to resolve many different types of logging issues.

Supported Operating Systems

All supported operating systems.

Supported Appliances

All supported appliances.

Supported Versions

All supported versions, including R70 and higher.

Impact on the Environment and Warnings

The potential impact depends on the troubleshooting steps. See the notes applicable to each step.

Troubleshooting Procedures

Preliminary Questions

These are some questions that you should ask before troubleshooting logging issues:

- Is this a new installation?
- Were the logs operating correctly before the issue started?
- What recent changes could possibly cause this issue?
- Does the Security Management server receive logs from many Security Gateways or from one Security Gateway?
- If the Security Management server receives logs from many Security Gateways, is the issue with all or only one Security Gateway?

The answers to these questions can help determine which troubleshooting steps are appropriate.
Note - You can resolve many logging issues simply by rebooting the Security Gateway or the Security Management server. You should always try rebooting before doing more complex troubleshooting procedures. Of course, if logging issues occur frequently, you should try these troubleshooting procedures.

Incorrectly Configured Standalone Deployments

A **standalone deployment** is where a Security Management server and Security Gateway are installed on the same computer. In a **distributed deployment**, the Security Management server is installed on one computer and the Security Gateways are installed on different computers.

Make sure that your Security Management server is not incorrectly configured as a standalone deployment. This can happen because of a configuration error during a new installation or by rebooting the Security Management server while it is still installing its initial policy.

To Change a Security Management server that is Incorrectly Configured as a Standalone Deployment:
1. Run `cpprod_util FwIsFireWallModule`. If the output value is 1, the Security Management server is incorrectly configured as a standalone deployment. Continue with this procedure.
2. Run `fw unloadlocal` to unload the policy from the Security Management server.
3. Run `cpprod_util FwSetFireWallModule 0` to disable the Security Gateway on this computer.
4. Reboot the computer.

The Security Management server is not in the Listening State

To Make Sure that the Security Management server is Listening on Port 257 (the Check Point Logging Port):
1. Run `netstat na` on the Security Gateway. If the Security Gateway is listening on port 257, the output should look similar to this example:
   
   TCP    10.1.1.13:257   10.1.1.2:2085     ESTABLISHED  
   TCP    10.1.1.13:257   10.1.1.3:1133     ESTABLISHED  
   tcp   0    0    10.1.1.2.2085    10.1.1.13.257   ESTABLISHED  

   In this example, the Security Management server (10.1.1.13) is listening to two Security Gateways (10.1.1.2, 10.1.1.3) on port 257. These two Security Gateways are in the LISTENING state and are sending logs.

Network Connectivity

To Make Sure that you Have Basic Network Connectivity:
3. Make sure that you have connectivity over port 257 and that firewall rules are not blocking this port. You can run `telnet mgmt_ip_address 257` to do this verification.

If you cannot ping or use telnet successfully, the traffic is probably being dropped or is incorrectly routed. You can use SmartView Tracker to identify dropped traffic or `tcpdump` ("Using tcpdump to Verify Network Connections" on page 7) to troubleshoot routing issues.
Installing a Policy

Make sure that you can install a policy on, or fetch a policy from the Security Gateway. If you cannot install or fetch a policy, make sure that SIC trust is operational between the Security Gateway and the Security Management server. Try reconfiguring SIC Trust.

To fetch a policy from the Security Management server, run `fw fetch <Security Management server host name or IP address>`.

Making Sure that Logs are Sent

If the log file is growing in size, it is likely that log files are not being sent to the Security Management server or the log server. To see if this is true, run these commands:

```
 cd $FWDIR/log
 ls -la
```

Run `netstat -an | grep 257` to show if the connection is established, but localhost destination is configured as the Security Gateway instead of the Security Management server or the log server IP address.

Verifying the Masters File

Make sure that the masters file (`%FWDIR/conf/masters`) contains the correct host name or IP address for the Security Management server or log server. The file should look similar to this:

```
fw[admin]# cat $FWDIR/conf/masters
[Policy]
 hostagae_of_FW
[Log]
 hostagae_of_FW
[Alert]
 hostagae_of_FW
```

If the host name or IP address does not match that of the Security Management server or the log server, you must correct this.

Using `tcpdump` to Verify Network Connections

This procedure lets you verify network connections between the Security Gateways and the Security Management server or log server.

To make sure that the gateway can send logs to the Security Gateway, run this command:

`tcpdump -i <interface connected to Security Management server> port 257`

To make sure that Security Management server can receive logs from the Security Gateway:

`tcpdump -i <interface connected to gateways> port 257`

You should see that the packet going from the Security Gateway is received by the Security Management server. Likewise, with the second command, you should see a packet going from the Security Management server to the Security Gateway.

`tcpdump` on interface connected to the Security Management server that is listening to port 257. This also shows the IP address that the Security Gateway is trying to send traffic to and from.

If you cannot see the packet going from one side to the other, do the network connectivity (on page 6) procedure.
Doing a Log Switch

Run `fw logswitch` on the Security Management server and then reboot the computer. If this does not resolve the issue, move the contents of the log directory ($FWDIR/log) to a temporary directory.

- Make sure that you do not copy the log directory itself.
- Make sure that the temporary directory is not a subdirectory of the log directory.

Reboot the computer and then check the logs.

Removing Possible Corrupted Files

To Remove Possible Corrupted Files:
1. Backup and then delete all log files ($FWDIR/log) on the Security Gateway.
2. Reboot the Security Gateway.
3. Look at the logs.

Using Debug

If none of these procedures helped you to resolve the issue, you can use the `debug` command to collect troubleshooting information. We recommend that you use debug with the `fwd` and `cpd` process on the Security Gateways and the Security Management server. Debugging the `cpd` process is useful for resolving SIC trust issues.

Suggested Workflow for Using Debug:
1. Run debug on the Security Gateway.
   ```
   cpd_admin debug on TDERROR_ALL_ALL=5
   fw debug fwd on TDERROR_ALL_ALL=5
   ```
2. Run debug on the Security Gateway.
   ```
   cpd_admin debug on TDERROR_ALL_ALL=5
   fw debug fwm on TDERROR_ALL_ALL=5
   fw debug fwd on TDERROR_ALL_ALL=5
   ```
3. Let debug run for 1 to 2 minutes and then stop the debug.
   ```
   cpd_admin debug off TDERROR_ALL_ALL=1
   fw debug fwm off TDERROR_ALL_ALL=1
   fw debug fwd off TDERROR_ALL_ALL=1
   ```
5. Send this information to customer support.

Verification

After each procedure, run SmartView Tracker to see if logs are received correctly from the Security Gateways.
Index

D
Doing a Log Switch • 8

H
How To Troubleshoot Logging Issues • 5

I
Impact on the Environment and Warnings • 5
Important Information • 3
Incorrectly Configured Standalone Deployments • 6
Installing a Policy • 7

M
Making Sure that Logs are Sent • 7

N
Network Connectivity • 6

O
Objective • 5

P
Preliminary Questions • 5

R
Removing Possible Corrupted Files • 8

S
Supported Appliances • 5
Supported Operating Systems • 5
Supported Versions • 5

T
The Security Management server is not in the Listening State • 6
Troubleshooting Procedures • 5

U
Using Debug • 8
Using tcpdump to Verify Network Connections • 7

V
Verification • 8
Verifying the Masters File • 7