How To Troubleshoot SIC-related Issues

11 January 2011
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=11880

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>1/9/2011</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 SIC-related Issues).
How To Troubleshoot SIC-related Issues

Objective

This document explains the steps for troubleshooting SIC failure scenarios with Check Point Security Gateway servers, both when initiating the SIC, and when testing its status at a specific time.

Supported Versions

- NGX R65 and oldest versions
- NGX R70
- NGX R71

Supported OS

- SecurePlatform

Supported Appliances

- Relevant for every appliance and open server
- For Open servers, refer to the Hardware Compatibility List in Check Point public site at:
  - http://www.checkpoint.com/services/techsupport/hcl/all.html
Before You Start

Related Documentation and Assumed Knowledge

There are several generic solution articles which can guide you when troubleshooting problems related to SIC issues.

Initially, go over:

- sk30579 - Troubleshooting SIC (http://supportcontent.checkpoint.com/solutions?id=sk30579)

If these do not solve your issue, go over the following flowchart:

Links to the SKs in the above diagram:

- A failure with initializing SIC:
  - sk12688 (http://supportcontent.checkpoint.com/solutions?id=sk12688)
  - sk35200 (http://supportcontent.checkpoint.com/solutions?id=sk35200)
  - sk25542 (http://supportcontent.checkpoint.com/solutions?id=sk25542)
  - sk37295 (http://supportcontent.checkpoint.com/solutions?id=sk37295)

- Getting the error "SIC General Failure":
  - sk37219 (http://supportcontent.checkpoint.com/solutions?id=sk37219)
  - sk32715 (http://supportcontent.checkpoint.com/solutions?id=sk32715)
  - sk16200 (http://supportcontent.checkpoint.com/solutions?id=sk16200)

- Error No. 300:
  - sk33906 (http://supportcontent.checkpoint.com/solutions?id=sk33906)
Impact on the Environment and Warnings

SIC relies on a process called CPD, meaning that while SIC operations are being performed (initiating SIC, testing SIC status, pulling a certificate from CA, etc.), CPD-related operations will also be executed.

The CPD process is responsible, among other things, for:

- Licensing
- Policy installation (Policy fetch)
- Secure Internal Communication (SIC)
- Status Report (AMON server for the SmartCenter Server)
- Implements a messaging mechanism for other SmartCenter Server daemons

In rare situations, CPD CPU usage can reach a high value during the debug procedure. If this happens, all CPD-related operations can be affected. This means they will be slower and can have performance issues for their specific purposes. Other than that, if the system is not extremely loaded, you should not experience any major impact on it.
Basic Information on SIC

Secure Internal Communications (SIC) is a certificate-based channel for communications between Modules. Check Point components communicate with each other using SIC.

The interaction between the Security Management server, the Firewall Gateway and other partner-OPSEC Applications must take place to ensure that the gateways receive all the necessary information from the Security Management server.

However, whereas information must be allowed to pass freely, it also has to pass securely. This means:

- The communication must be encrypted so that an impostor cannot send, receive or intercept communication meant for someone else.
- The communication must be authenticated, so that there can be no doubt as to the identity of the communicating peers.
- The transmitted communication should have data integrity (the communication has not been altered or distorted in any form).
- The SIC setup process allowing the intercommunication to take place must be user-friendly.

SIC relies on a process called CPD, which is responsible for performing all inter-module communications.

SIC is based on SSL with digital certificates. When the Management Server is installed, a Certificate Authority (CA) is created. This Certificate Authority issues certificates for all components that need to communicate to each other. For example, a remote FireWall-1 Module will need to have a certificate from the Management Server before a policy can be downloaded to this module, or before a license can be attached to the Module using SecureUpdate.

The purpose of the Communication Initialization process is to establish a trust between Security Management server and the Check Point gateways. This trust enables these components to communicate freely and securely. Trust can only be established when the gateways and the Security Management server have been issued SIC certificates. After successful Initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate, signed by the same ICA.

Management and Gateway Servers Synchronization

In order for the SIC between the Management and the Gateway servers to succeed, their clocks must be properly and accurately synchronized.

When the SIC certificate has been securely delivered to the gateway, the Trust state is: Trust Established.

The SIC status conveys whether or not the Security Management server is able to communicate securely with the gateway after it has received the certificate issued by the ICA. The most typical status is Communicating, and any other status indicates there is a problem with the SIC communication.

Communication takes place over the Check Point communication layer. This channel can therefore be encrypted in various ways. This layer can be called the SIC layer.

SIC layer provides a secure internal communication method between Check Point software entities.

- **Port 18209** is used for communication between the VPN-1/FireWall-1 Module and the Certificate Authority (status, issue, revoke).
- **Port 18210** is used to pull certificates from the CA.
- **Port 18211** is the port used by the cpd daemon on the Module to receive the certificate (when clicking Initialize in the Policy Editor).
Troubleshooting Procedures

In this section:

- Basic Troubleshooting Steps
- Checking Connectivity
- Checking CPD Memory Consumption
- Collecting the Debug

Basic Troubleshooting Steps

- Ensure connectivity between the gateway and Security Management server.
- Verify that server and gateway use the same SIC activation key.
- Check the date and time of the operating systems and make sure the time is accurate. If the Security Management server and remote gateway reside in two different time zones, the remote gateway may need to wait for the certificate to become valid.
- If the Security Management server is behind another gateway, make sure there are rules that allow connections between the Security Management server and the remote gateway.
- Ensure the Security Management server’s IP address and name, are in the `/etc/hosts` file on the gateway.
- If the IP address of the Security Management server undergoes static NAT by its local Security Gateway, add the public IP address of the Security Management server to the `/etc/hosts` file on the remote Security Gateway, to resolve to its hostname.
- Restart the CPD daemon with the following commands:

```
# cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"
# cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"
```

- Based on sk33764, using the command line of the gateway, type: `fw unloadlocal`. This removes the security policy from the Security Gateway server, hence all traffic is allowed through it.

Try again to establish SIC.
Checking Connectivity

Ensure that the SIC ports are open. As previously mentioned, the SIC ports are:

- **Port 18209** is used for communication between the VPN-1/FireWall-1 Module and the Certificate Authority (status, issue, revoke).
- **Port 18210** is used to pull certificates from the CA.
- **Port 18211** is the port used by the cpd daemon on the Module to receive the certificate (when clicking Initialize in the Policy Editor).

To determine if SIC is listening to its network ports on your Check Point device (can be Security Gateway server or Security Management Server), use the following command:

- **On Windows platforms:**
  - Open CMD and execute: `netstat -na | findstr 18211`
- **On Linux platforms:**
  - `netstat -na | grep 18211`
- **The output should be:**
  - `TCP 0.0.0.0:18211 0.0.0.0:0 LISTENING`

A NAT device between the SmartCenter Server and Security Gateway will not have any effect on the ability of a Check Point enabled entity to communicate using SIC, since the protocol is based on Certificates and SIC names (and not IPs).

To verify the Gateway is listening for the SmartCenter Server for getting certificates, the CPD debug output should be as follows:

```
[CPD ID]@cpmodule[Date] Get_SIC_KeyHolder: SIC certificate read successfully
[CPD ID]@cpmodule[Date] SIC initialization started
[CPD ID]@cpmodule[Date] get_my_sicname_from_registry: Read the machine's sic name: CN=member_1,O=cpmodule..6vxoys
[CPD ID]@cpmodule[Date] Initialized sic infrastructure
[CPD ID]@cpmodule[Date] SIC certificate read successfully
[CPD ID]@cpmodule[Date] Initialized SIC authentication methods
```

Checking CPD Memory Consumption

**High CPD Memory Consumption**

A memory leak is a particular type of unintentional memory consumption by a computer program (or daemon in Linux) where the program fails to release memory when it is no longer needed. In the case of a memory leak, memory usage steadily increases until no memory is left to be allocated. At this point, the process will crash and probably leave behind a core file that compiles the recorded state of the working memory of the daemon at the crashed time.

To ascertain that you are dealing with such a problem, monitor the 'top' command output in the involved servers while replicating the problem. (In case of a long-term leak, Check Point Support can also provide a special script that can be executed on the system and will collect this data at a constant interval).

While monitoring the 'top' command output, the necessary columns are:

- **RES (or RSS)** – For high memory consumption of specific process (for example – fwm).
- **%CPU** – For high CPU consumption.

It is also possible to sort this output, as follows - pressing:

- **M** – sorts the output based on the memory usage (RSS column).
- **P** – sorts the output based on the CPU usage (%CPU column).
Usually, when the server suffers from high memory consumption, the affected process will eventually crash, since (due to Linux limitation) it can only reach a memory consumption of ~2GB.

**To create the core file, enable the option of a core dump creation, as follows:**

On the server where the process crashes:

```
# um_core enable
# ulimit -c unlimited
# reboot
```

which provides the core file that will be generated after the next crash.

- The core file name should be similar to: `<proc_name>.<core_serial_number>.core`
- File should be created under `/var/log/dump/usermode`.

The process can crash immediately after performing the operation which is related for that process (means it it is not necessarily a leak, just large enough to cause a crash at a specific point). In such cases, the core dump file size can take few hundred MB, or after some time on which the memory usage for this process reaches the highest limit it is capable of, where the core dump file can take more than 2 GB.

Many high memory consumptions issues are solved on the HFA releases, therefore, if you encounter such an issue, try to install the latest HFA. If it is a known issue, the HFA will probably overcome it.

If the issue was not solved during the latest HFA, collect the core file (if it was created), together with the TOP command output that shows the high usage and send this information to Check Point support.

Since SIC operations are performed by the CPD daemon, the monitored process should be the CPD on both the Security Management server and the Security Gateway server.


---

**Collecting the Debug**

If none of the above steps solved your SIC issue, you will have to debug the scenario.

Because SIC relies on the CPD process, this is the relevant process to be debugged.

**To debug SIC-related scenarios:**

**Option 1**

1. Clean the old log file(s), by issuing:
   - `# rm $CPDIR/log/cpd.elg.*`
   - `# echo ' ' > $CPDIR/log/cpd.elg`
2. Start the debugging:
   - `# echo '====debug_start===' >> $CPDIR/log/cpd.elg`
   - `# cpd_admin debug on TDERROR_ALL_ALL=5`
   - `# cpd_admin debug on OPSEC_DEBUG_LEVEL=9`
3. Replicate the problem
4. Stop the debugging:
   - `# echo '====debug_stop===' >> $CPDIR/log/cpd.elg`
   - `# cpd_admin debug off TDERROR_ALL_ALL=0`
   - `# cpd_admin debug off OPSEC_DEBUG_LEVEL=0`
5. Debug output files, located at:
   - `$CPDIR/log/cpd.elg*`
Option 2

1. Stop the CPD process:
   - `# cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"

2. Enable the debug flags:
   - `# export TDERROR_ALL_ALL=5`
   - `# export OPSEC_DEBUG_LEVEL=9`

3. Start CPD on debug level:
   - `# cpd -d > cpd_debug.txt 2>&1`

4. Replicate the problem.
5. Issue CTRL+C to stop the 'cpd -d' debug.
6. Disable the debug flags:
   - `# unset TDERROR_ALL_ALL`
   - `# unset OPSEC_DEBUG_LEVEL`

The debug output file is `cpd_debug.txt` which is located on your current directory. These should provide an indication about the issue that causes the SIC failure. When finding a suspicious log entry within these files (look for error, fail, etc.), it is necessary to look for it on Secure Knowledge database (Check Point public site). If nothing similar is found, open a new Service Request with Check Point support and provide the information you collected.

For further debug information, please refer to sk41513

Completing the Procedure

- Make sure you have gone through all the steps in the Troubleshooting Procedures.

Verifying

To verify that the issue you encountered has been solved:
1. Check that SIC is established with the Security gateway. Go to the gateway object in SmartDashboard.
2. In the General Properties tab, under the Secure Internal Communication section, click Communicate.
3. In the opened window, click Test SIC Status.

   The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

If after going over the steps in this guide the SIC status is anything other than Communicating, contact Check Point support and open a new Service Request with all the relevant information collected in this procedure.