How To Troubleshoot Policy Installation Issues

28 September 2011

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

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=11844

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

Revision History

Date	Description
22 September 2011	Fixes to linked Secure Knowledge
December 2010	First release of this document

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 Policy Installation Issues).

Contents

How to Troubleshoot Policy Installation Issues

Objective

This document explains the steps for troubleshooting Policy Installation failures scenarios in SmartCenter and Security Management Servers. It refers to Policy Installation for Check Point Security Gateways

Supported Versions

This document is suitable for every SmartCenter and Security Management server.

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

Supported OS

- SecurePlatform

Supported Appliances

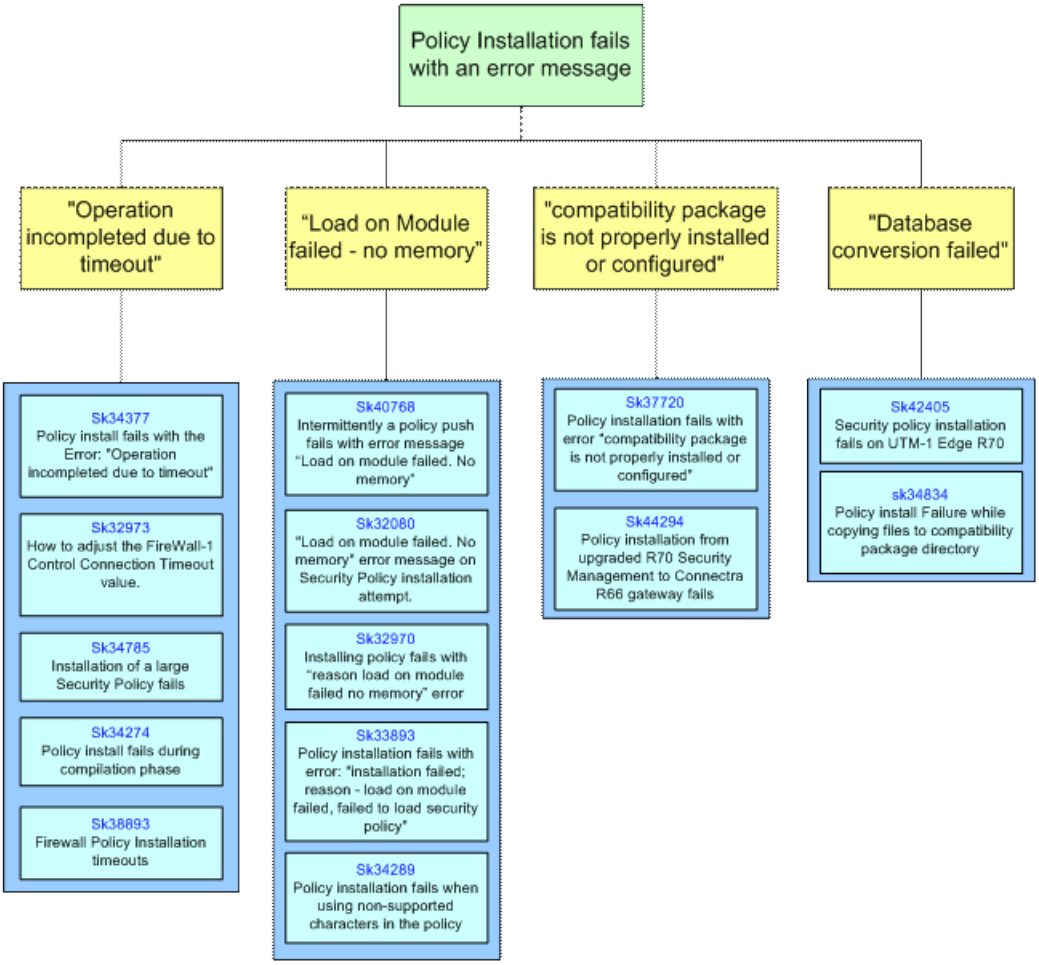
- Relevant for every appliance and open server

For open servers, see the Hardware Compatibility List in the Check Point public site (http://www.checkpoint.com/services/techsupport/hcl/all.html).

Before You Start

Related Documentation and Assumed Knowledge

There are several generic solution articles and documentations which can guide you when troubleshooting problems related to Policy Installation.



Links to the SKs in the above diagram:

- Operation incompleted due to timeout
  - sk34377 (http://supportcontent.checkpoint.com/solutions?id=sk34377)
  - sk32973 (http://supportcontent.checkpoint.com/solutions?id=sk32973)
  - sk34785 (http://supportcontent.checkpoint.com/solutions?id=sk34785)
  - sk34274 (http://supportcontent.checkpoint.com/solutions?id=sk34274)
  - sk38893 (http://supportcontent.checkpoint.com/solutions?id=sk38893)
- Load on Mudule failed - no memory
  - sk40768 (http://supportcontent.checkpoint.com/solutions?id=sk40768)
  - sk32080 (http://supportcontent.checkpoint.com/solutions?id=sk32080)
  - sk32970 (http://supportcontent.checkpoint.com/solutions?id=sk32970)
  - sk33893 (http://supportcontent.checkpoint.com/solutions?id=sk33893)
  - sk34289 (http://supportcontent.checkpoint.com/solutions?id=sk34289)
- Compatibility package is not properly installed or configured
  - sk37720 (http://supportcontent.checkpoint.com/solutions?id=sk37720)

  - sk44294 (http://supportcontent.checkpoint.com/solutions?id=sk44294)
- Database conversion failed
  - sk34834 (http://supportcontent.checkpoint.com/solutions?id=sk34834)

Impact on the Environment and Warnings

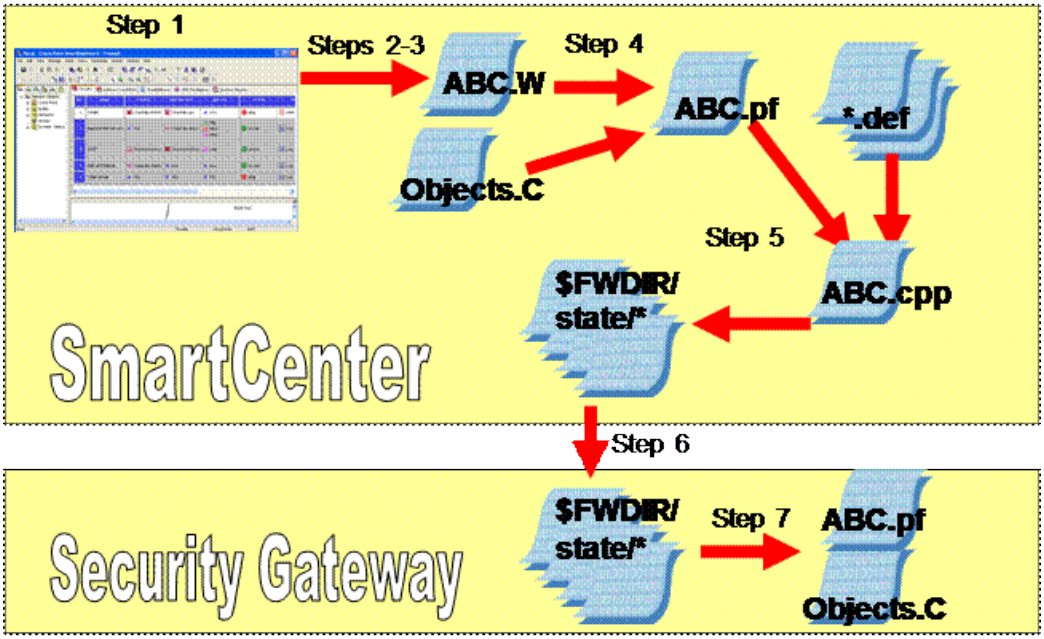
- The FWM process will be slower and have performance issues for management-related operations.
- There is no effect on the managed gateways.

Basic Information About the Policy Installation Process:

During the process commonly called "install policy" the following steps occur:

- **Initiation** - Policy installation is initiated with dedicated dialog window from SmartDashboard GUI (or from CLI). The information is passed from Smart Dashboard to the SmartCenter.
- **Verification** - The information in the database is verified to comply with a number of rules specific to the application and package, for which policy installation is requested. If this verification fails, the process ends here and an error message is passed to the initiator.
- **Conversion** - The information in the database is converted from its initial format to the format, understandable by further participants (GUI, SmartCenter, GWs, etc.). During conversion, rules that constitute security policy are put into result file named `<policy_name>.W`. This file, like the rest of converted and waiting for code generation data, resides in the `conf` sub-directory of the relevant compatibility package
- **Code generation and compilation** - Policy is translated to the INSPECT language and compiled with INSPECT compiler. The result of the code generation is a long string, containing resulting INSPECT source code, which is added into file named `<policy name>.pf`, which also resides in the `conf` sub-directory of the relevant compatibility package.
- The next step is creating "state directories" which is a file system directory where files are ready to be transferred to the module. A dedicated process compiles the `$FWDIR/conf/*.pf` with all the relevant `$FWDIR/lib/*.def` files and create a temporary file called `*.cpp` which is transferred to the "state directories".
- **CPTA** – Policy files are transferred (from the temporary state directories) and saved on the gateway side in the gateway's temporary state directory. Policy is transferred to the firewall gateway using SIC. It reads files from state directories into internal buffers and starts policy transfer to all the involved gateways.
- **Commit** – When all the files are transferred successfully, process called "commit" is initiated – firewall software is instructed to read the new security policy and start to use it. If everything went OK, `cpd` process on the gateway side saves the policy in the gateway's permanent state directory.

At this point, policy installation process end and the gateway is commanded to load the new policy.



Troubleshooting Policy Installation

In this section

SIC-related Issues

You can configure secure communication channels between Check Point nodes, using Secure Internal Communication (SIC). SIC makes sure that these nodes can communicate freely and securely.

To verify SIC-related issues:

- Make sure SIC is established between Management server and Security Gateway.
- Make sure the SIC ports are open - make sure there is connectivity between the nodes.

To check that SIC is established with the Security Gateway:

1. Go to the gateway object in SmartDashboard.
2. In the General Properties tab, under the Secure Internal Communication section, click **Communicate**.
3. In the window that opens, click **Test SIC Status**.

If the status of the server secure communication with the gateway is good, the SIC Status window shows:

SIC Status for *computer***: Communicating**

If the status is **Not Communicating**, there is a problem with SIC.

See sk30579 (http://supportcontent.checkpoint.com/solutions?id=sk30579), for:

- Troubleshooting basic SIC related issues.
- Troubleshooting SIC ports failures.
- Going over known SIC scenarios and common actions.

Connectivity

To check connectivity, ensure that the policy installation ports are open:

1. On the Management station issue the command:

   ```
   # netstat -na | grep 18191
   ```

   and ensure it is listening on port 18191, which is used by the CPD process for communications such as policy installation.
   The output from the management station should show something similar to:

   ```
   tcp     0    0 0.0.0.0:18191           0.0.0.0:*               LISTEN
   tcp     0    0 192.168.70.163:18191    192.168.70.162:52744    ESTABLISHED
   ```

   This means there is an established connection (due to the policy installation action) between the SmartCenter server (192.168.70.163) and the security gateway (192.168.70.162).

   In addition, verify that port 18191 is on listening in the Security gateway:

```
# netstat -na | grep 18191
tcp    0   0 0.0.0.0:18191           0.0.0.0:*               LISTEN
tcp    0   0 192.168.70.162:38566    192.168.70.163:18191    ESTABLISHED
```

2. Ensure that port 256 is also open for communication.
   When installing a policy, the management console uses this port to push the policy to the Security gateway module. On both devices, you should see the following:

```
# netstat -na | grep 256
tcp     0      0 0.0.0.0:256             0.0.0.0:*               LISTEN
```

High CPU Usage/Memory Consumption

In some circumstances, the install policy process fails due to high CPU or high usage of a specific process on one of the involved servers (Management server and/or Security Gateway).

To verify that you deal with such problems, monitor the 'top' command output on the involved servers while replicating the problem. During the policy installation process, the server consumes more memory than usual (especially `fwm` takes more memory and CPUusage), but, in case it does not free the necessary space after the operation is finished, policy installation may fail after a while (several days/weeks/months).

To troubleshoot high CPU usage or high memory consumptions on the involved machines:

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 possible also 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 it can reach (due to Linux limitation) a memory consumption of ~2GB. When a process crashes, it also creates a core file. However for this to happen, you must first enable the core file creation option.

To generate a core file:

On the server where the process crashes:

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

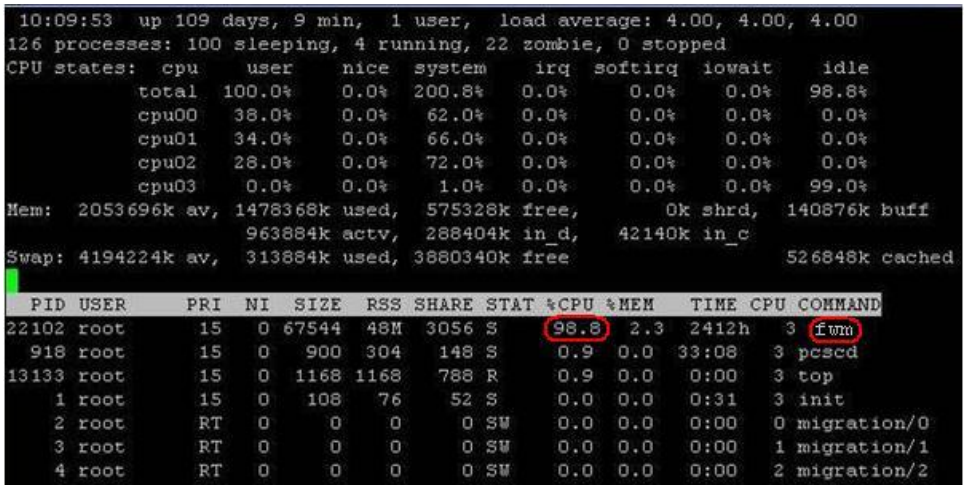
Provide the core file that will be generated after the next crash.

- Core file name should be like `<proc_name>.<core_serial_number>.core`
- File should be created under `/var/log/dump/usermode`

Many high CPU usage and high memory consumptions issues are solved on the HFA releases, therefore, if you encounter an issue that causes a policy installation failure, try to install the latest HFA. If it is a known issue, the HFA will probably overcome it.

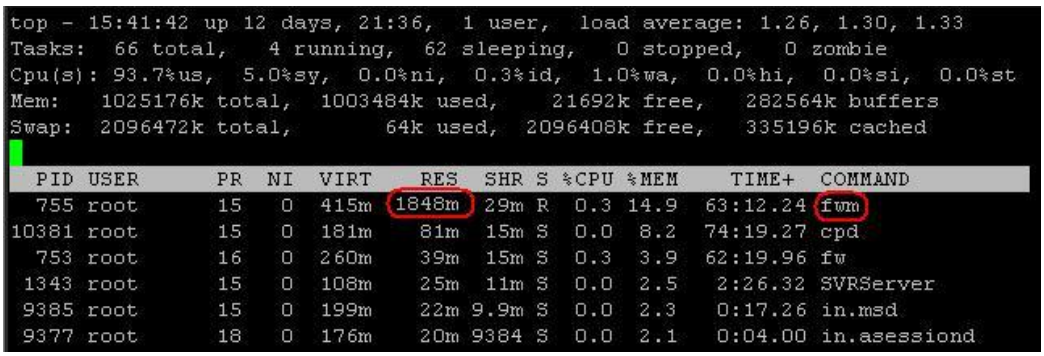
If the issue was not solved during the latest HFA, collect the core file (if it was created), together with the TOP command output that shows the high usage and send this information to Check Point support.

The screenshot below, gives an example for high CPU usage with the FWM process:



Refer to sk35496 (http://supportcontent.checkpoint.com/solutions?id=sk35496) to detect high memory consumption (memory leak) on your Security Gateway server.

The screenshotbelow shows an example for high memory consumption with the `FWM` process:



Verification/Compilation Stages

When installing a policy, the Installation Process window is displayed, allowing you to monitor the progress of the verification, compilation and installation.

- If the verification is completed with no errors and the Security Management server is able to connect to the gateway securely, the Policy installation succeeds.
- If there are verification or installation errors, the installation fails (see Installation Stage (on page 12)).
- If there are verification warnings, the installation succeeds with the exception of the component specified in the warning.

The failure can be due to two reasons:

- Failure is on the MGMT side - Installation fails on verification or compilation stages.
- Failure is on the GW side - Installation fails on Installation stage.

To troubleshoot Policy Installation process failure on Verification/Compilation stages:

Before starting to troubleshoot, please go over the following known and common scenarios:

- sk39935 (http://supportcontent.checkpoint.com/solutions?id=sk39935) - Policy installation failed on verification stage.
- sk34022 (http://supportcontent.checkpoint.com/solutions?id=sk34022) - Policy install fails with NAT error
- sk41682 (http://supportcontent.checkpoint.com/solutions?id=sk41682) - Policy verification error "No policy loader is defined for the target
- sk37214 (http://supportcontent.checkpoint.com/solutions?id=sk37214) - Installation policy failed on compilation with error message: "Failed to Download Security Policy on xxxx: Too many open files"

- sk34671 (http://supportcontent.checkpoint.com/solutions?id=sk34671) - INTERNAL ERROR in LenLimit: displacement too big 4081 (max = 4080) Compilation failed. Operation ended with errors. Cannot install policy
- sk33297 (http://supportcontent.checkpoint.com/solutions?id=sk33297) - Policy install fails due to empty valid_addrs_list tables

For failures on the MGMT side:

1. Try to install policy from the CLI by performing the following command (the command output should also be saved) on the MGMT server:
   ```
   # fwm -d load $FWDIR/conf/PolicyName.W <target>
   ```
   The target flag stands for the designated target on which the command will be executed.
   If the above command ended with a failure, go over the output and look for error, fail, etc.
2. Try to install policy from the Smart Dashboard and at the same time perform the following debug:
   On the Management (SmartCenter):
   - Clean the old log files:
     ```
     # cd $FWDIR/log
     # rm fwm.elg.*
     # echo ' ' > fwm.elg
     ```
   - Enable the FWM debug:
     ```
     # fw debug fwm on TDERROR_ALL_ALL=5
     # fw debug fwm on OPSEC_DEBUG_LEVEL=9
     ```
3. Replicate the problem by installing the policy from the SmartDashboard GUI.
   - To stop the FWM debug on the MGMT server, execute:
     ```
     # fw debug fwm off TDERROR_ALL_ALL=1
     # fw debug fwm off OPSEC_DEBUG_LEVEL=1
     ```

In the MGMT server, the debug (`fwm.elg*`) located under `$FWDIR/log/`. These debug outputs, together with the output of the installation from the CLI, should give an indication about the issue that causes the policy installation failure. If there are any suspicious log entry within these files (look for error, fail, etc.), look for it on Secure Knowledge database.

If nothing is found, send this information, together with the screenshot of the error to Check Point support.

Installation Stage

If there are verification or installation errors, the policy installation will fail. When installation fails at the Installation stage, it means that the failure is on the gateway side.

Common errors for this scenario are:

- "Installation failed. Reason: Load on Module failed - failed to load Security Policy."
- "Operation incomplete due to timeout"

For such error messages, please refer to the flowchart at the beginning of the guide which contains the necessary troubleshooting steps.

However, most of the errors occuring as the push policy process fails on the installation stage, are very generic and can be caused by a variety of problem.

To troubleshoot Policy Installation process failure on the Installation stage - on the gateway side:

Try to fetch the policy from the CLI by performing the following command (the command output should also be saved) on the problematic Security Gateway server:

```
# fw -d fetch <MGMT IP address>
```

If the above command ended with a failure, go over the output and look for error, fail, etc.

1. Try to install policy from the Smart Dashboard and at the same time perform the following debug:

a) On the Management (SmartCenter):

- Clean the old log files:

```
# cd $FWDIR/log
# rm fwm.elg.*
# echo ' ' > fwm.elg
```

- Enable the FWM debug:

```
# fw debug fwm on TDERROR_ALL_ALL=5
# fw debug fwm on OPSEC_DEBUG_LEVEL=9
```

b) On the enforcement module (the gateway):

- Clean the old log files:

```
# cd $CDDIR/log
# rm cpd.elg.*
# echo ' ' > cpd.elg
```

- Enable the CPD debug:

```
# cpd_admin debug on TDERROR_ALL_ALL=5
```

2. Replicate the problem by installing the policy from the SmartDashboard GUI.

- To stop the FWM debug on the MGMT server, execute:

```
# fw debug fwm off TDERROR_ALL_ALL=1
# fw debug fwm off OPSEC_DEBUG_LEVEL=1
```

- To stop the CPD debug on the Security gateway server, issue:

```
# cpd_admin debug off TDERROR_ALL_ALL=1
```

In the MGMT, debug (`fwm.elg*`) located under `$FWDIR/log/`, in the gateway, debug (`cpd.elg*`) located in `$CPDIR/log`. These debug outputs, together with the output of the installation from the CLI, should provide an indication about the issue that causes the policy installation failure. If there are suspicious log entry within these files (look for error, fail, etc.), look for it on Secure Knowledge database.

If nothing is found, send this information, together with the screenshot of the error to Check Point support.

Completing the Procedure

- While performing the steps described in this document for dealing with policy installation failures, you should have determined whether the issue is related to the Security Gateway or to the Security Management (SmartCenter) server.
- If the issue cannot be solved after going through these steps, the mentioned debug must be collected and analyzed. The debug should capture the problem, and give an indication of the trigger that caused the failure. This indication will probably be presented by specific error logs which are related to the main problem. While identifying these error log entries, further investigation should be performed and if these are known messages, they will be found on the Secure Knowledge database, in any other case, contact Check Point support.