Technical Configuration Example

Feature Automation Script—
time-based-filters.slax, cs-time-based-filters.slax

Automate activating firewall filters during specified time ranges.
This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, The Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. GateD is based on Kermit’s EGP, UC Berkeley’s routing daemon (routed), and DCN’s HELLO routing protocol. Development of GateD has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,590, 5,903,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,676,902, 6,578,186, and 6,590,785.

Copyright © 2009, Juniper Networks, Inc. All rights reserved. Printed in USA.
# Table of Contents

**time-based-filters.slax, cs-time-based-filters.slax**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>1</td>
</tr>
<tr>
<td>System Requirements</td>
<td>1</td>
</tr>
<tr>
<td>What it Does</td>
<td>1</td>
</tr>
<tr>
<td>Set Up</td>
<td>1</td>
</tr>
<tr>
<td>Example</td>
<td>3</td>
</tr>
<tr>
<td>Notes and Restrictions</td>
<td>4</td>
</tr>
<tr>
<td>How to Run</td>
<td>5</td>
</tr>
</tbody>
</table>
time-based-filters.slax, cs-time-based-filters.slax

Description
When a time-based event script is used in tandem with a commit script, the configuration required for the event script can be created immediately without waiting for the event to occur. This automates activating firewall filter terms during specified time ranges. This is used to create a time-based stateless firewall filter.

System Requirements
The minimum JUNOS version is 9.3. Additionally, this script is only supported on the following JUNOS releases:
- 9.3R5
- 9.4R4
- 9.5R3
- 9.6R2

What it Does
The event script time-based-filters.slax and the commit script cs-time-based-filters.slax are paired to create time-based stateless firewall filters. The scripts employ user-defined arguments from the router configuration to automatically activate and deactivate specified filter terms at designated periods. The user loads the script files, enables them, and marks the filter terms with appropriate macros that provide instructions regarding the times when the firewall terms should be enabled or disabled.

Set Up
1. Copy the script time-based-filters.slax to the /var/db/scripts/event directory on the router.
2. Copy the script cs-time-based-filters.slax to the /var/db/scripts/commit directory on the router.
3. Enable the scripts by adding the file statement and script filename to the appropriate hierarchy level for the script type. Only superusers can enable scripts in the configuration.

   [edit event-options event-script]
   user@host# set file time-based-filters.slax

   [edit system scripts commit]
   user@host# set file cs-time-based-filters.slax

    NOTE: On dual-routing engine (dual-RE) systems you need to perform all of the initial steps on each of the routing engines—you must copy the scripts to their respective directories and enable both the event script and the commit script on each routing engine.

4. Add time-range configuration macros to any firewall filter term that should be enabled or disabled at specific times. These are added by entering the apply-macro statement under the firewall filter term hierarchy, with a macro name of either active-time-range or inactive-time-range.
The basic outline of the time-range macro is:

   term <rule-name> {  
      apply-macro (active-time-range | inactive-time-range) {  
         start-time <start-time>;
         stop-time <stop-time>;
      }
   }

   NOTE: Macros are a simple way to embed user-defined syntax, e.g. a name-value pair, inside JUNOS configuration.

5. To add a macro, enter the configuration mode on the routing device, navigate to the hierarchy of the firewall filter that should be time-based, and add the desired time-range macro with the time-range defined.

6. The default state for the firewall filter term will be the opposite of the time-range state designated in the macro. For example, if an active-time-range is specified for a firewall term, the term will be set to inactive by default unless the current time falls within the active-time-range that is specified. Within a time-range macro, both the start-time and stop-time statements must be configured to specify the start of the active/inactive period.

   Time is specified in one of the formats listed below, where HH is in 24 hour format, and MM can only be 00, 15, 30, or 45.

   - HH:MM - The time applies to every day at the HH:MM specified.
   - weekdays HH:MM - The time applies to only weekdays at the HH:MM specified.
   - weekends HH:MM - The time applies to only weekends at the HH:MM specified.
   - mon HH:MM - The time applies on the day of the week (sun, mon, tue, etc) at the HH:MM specified.
Example

For example, assume you want to set a family inet filter with the filter name re-protect to be time-based. You could do this by following these steps:

1. Enter configuration mode and navigate to firewall family inet filter re-protect:

   user@host> configure
   Entering configuration mode

   [edit]
   user@host# edit firewall family inet filter re-protect

2. Add the time-range macros to the filters. The example below creates a term rule called block-html that sets the active range of the filter from 8 a.m. to 5 p.m:

   [edit firewall family inet filter re-protect]
   user@host# set term block-html apply-macro active-time-range start-time 08:00

   [edit firewall family inet filter re-protect]
   user@host# set term block-html apply-macro active-time-range stop-time 17:00

Use the following examples of firewall filter terms with configured time-range macros to determine how to set up your own time-range macros. The term name is user-defined:

- This filter term will only be active from 8:00 a.m. to 5:00 p.m.:

  term day-term {
    apply-macro active-time-range {
      start-time 08:00;
      stop-time 17:00;
    }
    ...
  }

- This term will be inactive from 3:00 p.m. to 6:00 p.m.:

  term not-afternoon-term {
    apply-macro inactive-time-range {
      start-time 15:00;
      stop-time 18:00;
    }
    ...
  }

- This term will be active from Monday to Wednesday from 12:00 a.m. to 12:00 a.m. (24:00):

  term multiple-days {
    apply-macro active-time-range {
      start-time "mon 00:00";
      stop-time "wed 24:00";
    }
    ...
  }
This term will be active from 5:00 p.m. to 8:00 p.m. on weekdays:

```slax
term night {
    apply-macro active-time-range {
        start-time "weekdays 17:00";
        stop-time "weekdays 20:00";
    }
    ...
}
```

3. When finished setting up time-range macros, commit the configuration changes:

```
[edit]
user@host# commit and-quit
```

**Notes and Restrictions**

Below are restrictions to be aware of when using time-range macros and the time-based scripts in this section. These are in addition to the system requirements restrictions listed previously.

- Only the Coordinated Universal Time (UTC) time-zone is supported. If a different time-zone is configured the commit will fail with an error.
- You cannot include both `active-time-range` and `inactive-time-range` for the same term. Multiple ranges of the same type can be included by appending `-#` to the end to distinguish each range. (e.g. `active-time-range-1`, `active-time-range-2`, etc.)
- These configuration elements are reserved for use by the time-based filter script:
  - `groups time-based-filters-group`
  - `event-options generate-event time-based-filters-event`
  - `event-options policy time-based-filters-policy`
- A maximum of 10 unique HH:MM times can be configured, including `[event-options generate-events]`. If you try to configure more than 10, a commit error will result.
- Ensure that all filter terms are not deactivated at the same time; if they are, commit will fail.
- Counters in a time-based term lose their value when the term is deactivated.
- If your system time is ever manually changed, you must do one of the following to ensure that time events are on the correct time:
  - `commit full`
  - `restart event-processing or`
  - `request system scripts event-scripts reload`
- On a dual routing engine (dual-RE) system, time must be synchronized between the two REs. It is recommended that both REs be synchronized to an NTP server.
**How to Run**

The time-based filter script will run automatically at the start and stop times specified and will activate or deactivate the firewall terms whose state should be changed based on the start and stop times specified in the time-range macros in the configuration.

Term activations or deactivations will result in a syslog message to the external facility with a severity of info, for example:

- Jul 30 13:51:02 r2d2-re0 cscript: time-based-filters script activating term weekdays
- Jul 30 13:51:02 r2d2-re0 cscript: time-based-filters script deactivating term default