

Table of Contents

| | |
|---|---|
| Table of Contents | 1 |
| Detecting Dead Rules in Check Point firewall rule bases | 2 |
| House keeping | 2 |
| Limitations | 3 |
| Notice | 4 |

Detecting Dead Rules in Check Point firewall rule bases

i2drd is a simple system aiming to detect unused rules in a Check Point firewall rule base. This version is compatible with GAIa and has been tested on R77.10, R77.20 and R77.30, and should work with all later R77.x versions. It may work with other versions: the rule base format and the log file format is detected and the required information available from R65 and onwards, but the web server configuration requires R77.

UNIfw1lr is free software and released under a [modified BSD License](#), see LICENSE. Using the software requires a valid support contract with [Check Point Technologies](#).

i2drd is installed as an [rpm package](#) and the installation and configuration is described in

`INSTALL.md`.

The system consist of the following components:

- A Web-server: the system uses the [apache web server](#) supplied and maintained by Check Point, as part of the base operating system
- A collection of applications for parsing the *rule base*, extracting information from the *exported logfile* etc.

Access to the web-server is controlled by the firewall. The server runs on **TCP port 8088**. This may be changed in `/var/opt/i2drd/etc/drd` but is not recommended.

Log files are exported on a daily basis at midnight as configured in **UNIfw1lr**.

Processing the rule base and log file in order to detect unused rules starts at 13:59. This may change in the future.

All rules has a unique *UUID* which is logged. **i2drd** reads the log file and the rule base and counts the number of hits for each *UUID*. The result is written to a database and includes the last time a rule had a hit.

The date and time of the first time **i2drd** runs is recorded.

House keeping

- Inactive rules are not used actively in the rule base and are marked with **this color(orange)**. They may be deleted unless they serve any other purpose (e.g. documentation).
- Rules with no hits since *first run* are marked with **this color(pink)**. If *logging is disabled on the rule* then consider deleting the rule: it does not serve any firewall purpose.
- Rules without hits today are marked with this color (pale yellow) and should be checked firmly. The date the rule was last used and the number of days since then is in the report.

An example is shown here:

| | | | | | | | | | | | |
|--|----|----------|-------|--------------------|--|---------------------------|---|---------|--------|---------|--|
| 192.168.112.1 | | | | | | | | | | | |
| 0010 23:59:12 4ADD-9270-D693411102E) | | | | | | | | | | | |
| enabled | 23 | 030-0020 | 93 | 15Jun2016 22:12:09 | (F6C05E44-92D7-4809-8287-84C01F76D1D6) | Any | N_HVK_LAN | Any | drop | Log | Deny everything to LAN in Hvidovre |
| 040 - Server LAN | | | | | | | | | | | |
| enabled | 24 | 040-0010 | 217 | 15Jun2016 23:59:06 | (2FBF604D-996B-4D23-9546-D10653471D7D) | N_VM_DMZ-192.168.100.0-24 | Any | URL_log | Top | Account | Allow everything from server LAN in M1 and VM server LAN network in M1 |
| enabled | 25 | 040-0010 | 1022 | 10Sep2015 15:22:32 | (40E48F9A-92FF-43F3-94C0-30F8C05D077) | N_M1_SHVR_LAN | Any | Any | accept | Log | Allow everything from server LAN in M1 and VM server LAN network in M1 |
| enabled | 26 | 040-0010 | 36506 | 15Jun2016 23:59:06 | (004C5732-279D-4314-8081-51E3DFA2D786) | N_VM_DMZ-192.168.100.0-24 | Any | Any | accept | Log | Allow everything from server LAN in M1 and VM server LAN network in M1 |
| enabled | 27 | 040-0020 | 33 | 27Mar2016 22:32:19 | (D0BA753E-D2CA-4A7C-851D-0EDC8C00F839) | Any | N_M1_SHVR_LAN N_VM_DMZ-192.168.100.0-24 | Any | drop | Log | Deny all traffic to server LAN and VM server LAN network in M1 |
| vmware management network | | | | | | | | | | | |
| enabled | 28 | | 10 | 23Sep2015 3:15:36 | (883BCD31-0675-487E-AE81-8F3514F0816E) | G_M1_eth1_antispoof | Any | Any | accept | Log | Allow everything from ESXi hypervisor management network |
| enabled | 29 | | 1024 | 21Jan2015 11:02:35 | (A5E57698-4A23-44F4-8C03-36573088F964) | Any | G_M1_eth1_antispoof | Any | drop | Log | Deny everything to ESXi hypervisor management network |
| 050 - WEB DMZ | | | | | | | | | | | |
| enabled | 30 | | 1336 | 14Jun2016 23:55:37 | (73D6EFA2-3CDD-417D-8FFD-40786771D329) | N_WEB-DMZ-192.168.80.0-24 | G_Internet | Any | accept | Log | Allow everything from WEB DMZ to Internet |
| disabled | 31 | 050-0010 | 0 | aldrig | (F6B03ED4-99FC-4B03-8261-EDA29C058445) | WEB_SERVER-192.168.80.80 | Any | Any | accept | Log | Allow outgoing to ANY from web-server |
| enabled | 32 | | 218 | 14Jun2016 23:56:31 | (900F7E0A-3B69-4C28-89C0-143169216E9E) | dynobj | WEB_SERVER-192.168.80.80 WEB_SERVER-FF0580 | Any | drop | Log | Notice that dynobj MUST NOT BE EMPTY as it then matches Any |
| enabled | 33 | 050-0020 | 136 | 15Jun2016 23:48:21 | (D14D13F9-A1D5-48F9-97ED-437C68062F98) | Any | WEB_SERVER-192.168.80.80 WEB_SERVER-FF0580 | http | accept | Log | Allow specific services to WEB servers in DMZ |
| 055 - Inet rules -- directly connected hosts | | | | | | | | | | | |
| enabled | 34 | | 11 | 14Jun2016 22:00:01 | (3280F9C5-7DF3-4E95-A899-1155A53C4D48) | G_M1_eth1.200-antispoof | Any | URL_log | Top | Account | Rules for firewall testing - pfsense |
| enabled | 35 | | 282 | 14Jun2016 23:53:55 | (DF50C27C-CASC-4713-9165-9B1A9ADAC814) | G_M1_eth1.200-antispoof | Any | Any | accept | Log | Rules for firewall testing - pfsense |
| enabled | 36 | | 718 | 15Jun2016 | (30321C28-3A72-4040-4040-404040404040) | Any | pfsense | Any | accept | Log | Responsible monitor |

Limitations

The scope of the application are *rules*, not the *individual sources*, *destinations* and *services* which makes up a rule.

Assume there is 100 hits on the rule below, which has 3 sources, 2 destinations and two services.

| Nr. | Source | Destigation | Service |
|-----|--|------------------------------------|--------------|
| 1 | internal_mail_1 internal_mail_2 monitor_host_1 | external_mail_1 external_mail_2 | SMTP ICMP |

As we only know the hit count it is only possible to conclude that the rule is in use. It is however *not possible* to determine which network and service objects is used.

It may be that `monitor_host_1` is monitoring `external_mail_2` with `ICMP Echo Request` while no mail is processed.

The same goes for *group objects*, *ranges* and *networks*: one single host may be responsible for all traffic.

Proceed with care.

Notice

The package **i2drd** will be merged with **UNIfw1lr** (UNI•C firewall-1 log rotation) in the not so near future (don't hold your breath).

It is important to write documentation and guidelines as an integrated part of the software development process. So this documentation is made using common software tools and organised as text files written in [vi](#), saved as github flavored [markdown](#), controlled by a [makefile](#) and converted to [html](#) and [pdf](#) with [discount](#) and [wkhtmltopdf](#). Everything kept and controlled in [git](#).

The silly front page is made with a Mac application, saved as pdf and processed with `pdfunite`. Just for fun, and finished [in shorter time than going shopping in Fakta](#).