# Best Practices - Rulebase Construction and Optimization



| | |
|---|---|
| Solution ID | sk106597 |
| Product | Security Management, Multi-Domain Management / Provider-1, Security Gateway, ClusterXL, Cluster - 3rd party, VSX, SecureXL |
| Version | R75, R76, R77, R77.10, R77.20, R77.30, R80 |
| Platform / Model | All |
| Access Level | General |
| Date Created | 13-Jul-2015 |
| Last Modified | 27-Feb-2017 by david kornfeld |
| Status | Approved by TAC |
| Sr # | |
| Cr # | |
| Originator | Joseph Balazs |
| Editor | david kornfeld |
| Technical Resource | Peter Domotor |
| Last Approver | davidk@checkpoint.com |

## Solution

This article provides best practice guidelines for Check Point rulebase construction and optimization.

## Rulebase Overview

- The Check Point rulebase contains the policy rules that govern what connections are permitted through the firewall. When the firewall receives the first packet of a new connection it inspects the packet and checks the rulebase to see if the connection is allowed or if it should be either rejected or dropped.
- The rulebase is checked top-down meaning the firewall checks the rulebase by looking for a match in the first rule and if the connection is not matched the firewall then works its way down through the rulebase until it eventually finds a match.
- Rule order is a critical aspect of an effective rulebase because it can affect both the operational performance of the firewall and the operative accuracy of the policy. Having the same rules, but putting them in a different order, can radically alter the effectiveness of the firewall. Always place more specific rules first and the more general rules last to prevent a general rule from being applied before a more specific rule.

## General Rulebase Layout

The rules within the rulebase are generally arranged as shown below:

| |
|---|
| First rules |
| VPN rules |
| Authentication to Gateway rules |
| Admin and Management rules |
| Noise rule |
| Stealth rule |
| Business related rules |
| Before Last rules |
| Clean-up rule |
| Last rules |
| Drop rules |

- **The Business related rules section contains the rules that regulate your business traffic.**
  Business related rules should be grouped together in logical sub-sections to make the format of the rulebase easy to understand. The sub-sections that are most heavily used should be placed highest in the rulebase (so long as doing this does not compromise SecureXL tuning).

- **The blue coded rules are the Implied Rules (Policy > Global Properties > Firewall Implied Rules).**
  The enabled default Implied rules can be selectively turned off if not required or if the administrator has created specific rules to replace them. This is often done to harden or 'nail-down' the rulebase.

- **The green coded rules are VPN, management and noise rules.**
  The admin and management rules control access to the firewall e.g. SSH, HTTPS etc. If the implied rules have been disabled then specific rules to permit all require connections to and from the firewalls will be required.

- **The purpose of the Noise rule is to drop unwanted traffic such as NetBIOS traffic as high up in the rulebase as possible.**
  The use of a Noise rule helps to make the firewall more efficient by dropping unwanted traffic high up in the rulebase instead of at the bottom of the rulebase (clean-up rule).
  If the 'noise' traffic is mixed with 'useful' traffic then additional noise rules can be placed within the Business related rules section to drop the unwanted noise traffic once the useful traffic has been matched.

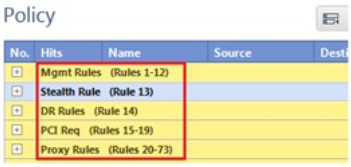
- **The Stealth rule should be located as early as possible in the policy, typically placed immediately after the management rules.**
  The purpose of the Stealth rule is to drop unauthorized connections destined to the firewall; protecting the firewall from being scanned and attacked.
  The rulebase is likely to be constantly evolving so the effectiveness of the Stealth rule should be periodically tested; it may need to be re-positioned to maintain effectiveness.

- **The clean-up rule is the last rule in the rulebase and is used to drop and log explicitly unmatched traffic.**
  To improve the rulebase performance, noise traffic that is logged in the Clean-up rule should be included in the Noise rule so it is matched and dropped higher up in the rulebase.

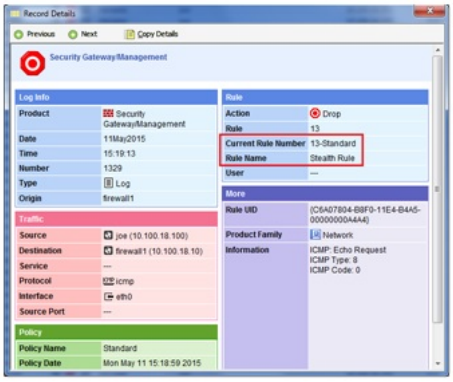
## Rulebase Best Practices

As the rulebase grows in length and complexity it becomes harder to understand and maintain. If several firewalls are managed by the same rulebase the complexity of the rulebase is further increased. Creating a single policy per firewall or firewall cluster can help to simplify the rulebase and make the policy easier to maintain.

- **Section Titles**
  Use section titles to identify and group similar rules together; makes the rulebase easier to understand and maintain. Section titling helps administrators to place additional rules in the right place within the policy.




- **Name Field**
  Use the Name field to create a name for the rule that describes the purpose of the rule. The name will appear in the logs and can help in troubleshooting sessions.


- **Comment Field**
  Use this field to further describe the rule and other pertinent information such as change request numbers.


## Rulebase Optimization

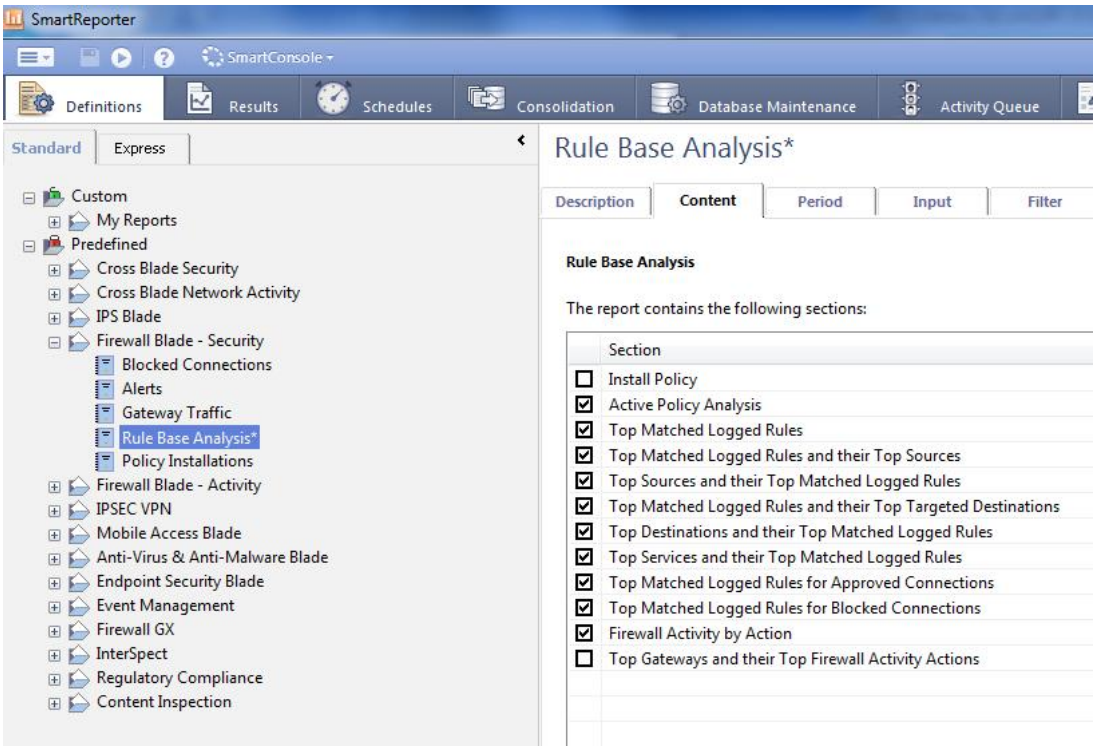
The rulebase efficiency is optimized by moving the most hit rules towards the top of the rulebase. Identifying the most hit rules can be achieved by using either the SmartReporter Rulebase Analysis report; the rulebase Hits count or by monitoring the Top Security rules in SmartView Monitor.

Some services and rulebase objects disable SecureXL or stop connection rate templating which will have a negative impact on the firewall's performance. It is important tc check moving a rule does not have a detrimental impact on SecureXL otherwise the benefit of moving the rule can be easily out-weighed by the impact on SecureXL.

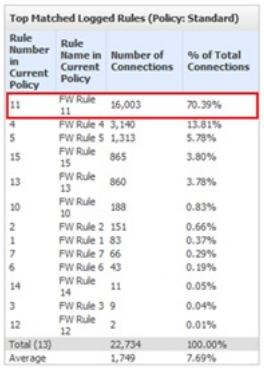
Refer to sk32578 (SecureXL Mechanism) to allow more connections to be accelerated by SecureXL.

**Identifying the Most Hit Rules:**

- **SmartReporter - Rulebase Analysis:**
  SmartReporter can provide a Rulebase Analysis report for individual firewalls based on logged traffic

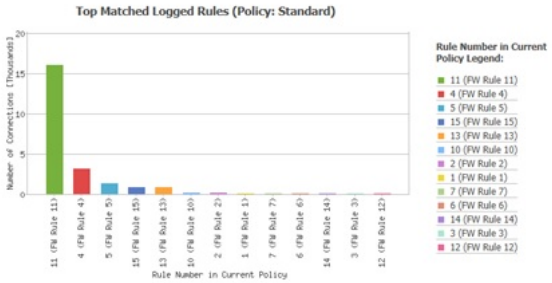



An extract from the Rulebase Analysis report:



Top Matched Logged Rules (Policy: Standard)

| Rule Number in Current Policy | Rule Name in Current Policy | Number of Connections | % of Total Connections |
|---|---|---|---|
| 11 | FW Rule 11 | 16,003 | 70.39% |
| 4 | FW Rule 4 | 3,140 | 13.81% |
| 5 | FW Rule 5 | 1,313 | 5.78% |
| 15 | FW Rule 15 | 865 | 3.80% |
| 13 | FW Rule 13 | 860 | 3.78% |
| 10 | FW Rule 10 | 188 | 0.83% |
| 2 | FW Rule 2 | 151 | 0.66% |
| 1 | FW Rule 1 | 83 | 0.37% |
| 7 | FW Rule 7 | 66 | 0.29% |
| 6 | FW Rule 6 | 43 | 0.19% |
| 14 | FW Rule 14 | 11 | 0.05% |
| 3 | FW Rule 3 | 9 | 0.04% |
| 12 | FW Rule 12 | 2 | 0.01% |
| Total (13) | | 22,734 | 100.00% |
| Average | | 1,749 | 7.69% |




- **Hits Counter:**
  The Check Point rulebase Hits counter (introduced in R75.40) shows the accumulated hits a rule has received in the rulebase. The rulebase hit count can be reset using the procedure in the following Secure knowledge article:

sk72860 (How to reset the 'Hit Count' in SmartDashboard)

Hit counter in the rulebase:

Policy

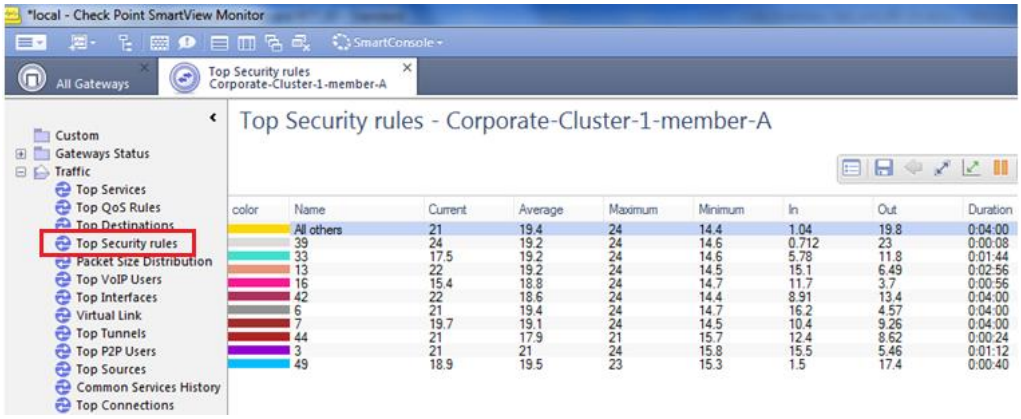
Search for IP, object, action, ...

| No. | Hits | Name | Source | Destination | VPN | Service | Action | Track |
|---|---|---|---|---|---|---|---|---|
| | Limit Access to Gateways Rule (Rule 1) | | | | | | | |
| 1 | 29K | VPN Stealth | Corporate-inte | GW-group | Any Traffic | Any | drop | Alert |
| | VPN Access Rules (Rules 2-5) | | | | | | | |
| 2 | 392K | Site to site VPN | Any | Any | All_GwToGw | CIFS<br>ftp-port<br>http<br>https<br>smtp | accept | Log |
| 3 | 0 | Remote access | Mobile-vpn-us | Any | RemoteAccess | CIFS<br>http<br>https<br>imap | accept | Log |
| 4 | 2K | Clientless VPN | Clientless-vpn- | Corporate-WA- | Any Traffic | https | User Auth | Log |
| 5 | 21K | Web server | L2TP-vpn-user@<br>Customers@Ar | Remote-1-web- | Any Traffic | http | accept | Log |
| | Rules for Specific Sites (Rules 6-8) | | | | | | | |
| 6 | 2M | Outbound HTTP | Remote-2-inter | Any | Any Traffic | http | Client Auth | Log |
| 7 | 640K | Critical subnet | Corporate-inte | Corporate-fina<br>Corporate-hr-n<br>Corporate-rnd- | Any Traffic | Any | accept | Log |

- **SmartView Monitor - Top Security rules:**
  If the firewall's monitoring blade is active then SmartView Monitor can be used to monitor the most hit firewall rules.

  Monitoring blade option on Firewall object (license required):


SmartView Monitor - Top Security rules:




## SecureXL and Rule Placement

Some factors, such as certain operations and IPS defenses may decrease SecureXL performance, resulting in loss of traffic acceleration, disabled templates and a decreased session rate. Optimizing the rulebase for SecureXL will help to optimize the performance of the firewall.

Refer to sk32578 (SecureXL Mechanism).

## Rulebase Installation Performance

Unused objects and duplicate objects will increase the policy verification time. Avoid creating duplicate objects and delete unnecessary objects. Cleaning up these objects can greatly improve the overall policy installation time.

Check Point Professional Services can assist with identifying the unused and duplicate objects and can create a custom scripts to clean-up the objects.

## Related documentations

- Security Management Server Administration Guide (R75, R75.20, R75.40, R75.40VS, R76, R77)
- Multi-Domain Security Management Administration Guide (R75, R75.20, R75.40, R75.40VS, R76, R77)
- Command Line Interface Reference Guide (R75, R75.20, R75.40, R75.40VS, R76, R77)

**Related Solutions**

sk102812 - Best Practices - Firewall Policy Management

This solution has been verified for the specific scenario, described by the combination of Product, Version and Symptoms. It may not work in other scenarios.

## Comments for Internal users only

**(October 6, 2015) General as per Uri Lewitus.**

Give us Feedback **Please rate this document** [1=Worst,5=Best]

**Comment** Enter your comment here Submit