Best practice web filtering - large scale

Report present to:
SE

Prepared by:
David Pigeon
SE

DATE
December 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

Tables of Contents

Best practice web filtering - large scale

Challenges

The challenge when installing Check Point into a new environment is that the firewalls are tune up or optimized by default for an environment around 1000 to 2500 users. When deploying Check Point into bigger environment consultant or customer will face issues at certain point in time.

This document is meant to address issues proactively regarding URL Filtering and Application Control which might need some special attention.

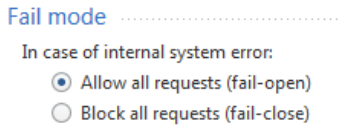
For general best practices documentation please refers to sk111303.
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111303&partition=General&product=All%22

Important daemons or services responsible to the well-being of URLF

- **RAD**: Resource Advisor – Responsible for the detection of Social Network widgets and the categorization of URLs. The detection is done via requests to ThreatCloud database, which identifies URLs as applications.
    - Path: *$FWDIR/bin/rad*
    - Commands: *# rad_admin stop|start*
    - Notes: "*cpwd_admin list*" command shows the process as "RAD".
- **usrchkd**: Main UserCheck daemon, which deals with UserCheck requests (from CLI / from the user) that are sent from the UserCheck Web Portal.
    - Path: *$FWDIR/bin/usrchkd*
    - Commands: start or stop via "*cpstop*" and " *cpstart*"
    - For restart use *# killall userchkd*
    - Notes:
        - This daemon is not monitored by Check Point WatchDog ("*cpwd_admin list*")
        - This daemon is spawned by the FWD daemon

RAD categorization request sessions

By default the RAD services will send one request to ThreatCloud for categorization per session. In large environment that could lead to a lot of sessions and it might crash the daemon. When the RAD daemon crashed the decision is made by the Fail mode configuration as fail-open or fail-close.



For R77.30 and below it does require a hotfix. For R80.10 and R80.20 the fix is already there it just require tune up.

Please consult the sk103422 the values could be change from 1 to 40

1. Configure the number of RAD queries per connection to a value between 20 and 40:
Note: If no value is configured, then default value of 1 query per connection will be used.

[Expert@HostName:0]# ckp_regedit -a SOFTWARE\\CheckPoint\\FW1\\$(cpprod_util CPPROD_GetCurrentVersion FW1) RAD_QUERIES_NUMBER_PER_CONNECTION <number>

Example:
[Expert@HostName:0]# ckp_regedit -a SOFTWARE\\CheckPoint\\FW1\\$(cpprod_util CPPROD_GetCurrentVersion FW1) RAD_QUERIES_NUMBER_PER_CONNECTION 30

2. Verify that the new attribute was added to registry:

[Expert@HostName:0]# grep --color -C 1 RAD_QUERIES_NUMBER_PER_CONNECTION $CPDIR/registry/HKLM_registry.data

3. Reboot the machine

RAD categorization buffer

Each gateway have a cache where it store the categorization of URLs, it will search the cache before doing a request to the cloud. The URL Filtering cache limit default value is 20 000, which is usually enough for a Security Gateway holding 1000 users. CPU utilization will rise if we have more users behind the firewall. The cache entries will reset to 0 when it reach it maximum value. Maximum value is 400 000!

How to check the current number of entries in the URL Filtering cache?

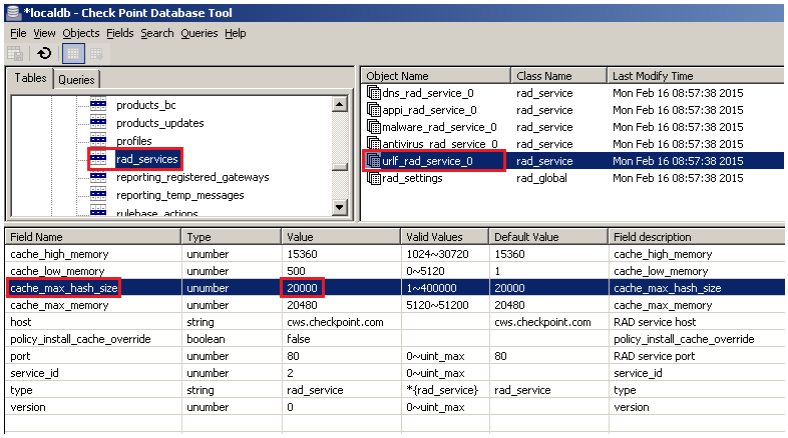
On the Security Gateway / each cluster member, run the ***fw tab -t urlf_cache_tbl -s*** command (in Expert mode) and look at the ***#VALS*** column, which shows the current number of entries in the cache.

Example:
[Expert@HostName]# fw tab -t urlf_cache_tbl –s

HOST	NAME	ID	#VALS	#PEAK	#SLINKS
localhost	urlf_cache_tbl	*XXX*	**1723**	0	0

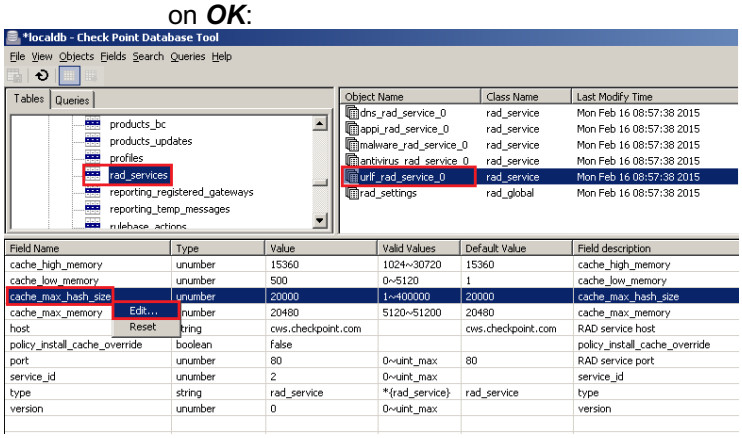
How to check the current limit of the URL Filtering cache?

1. Connect to Security Management Server / Domain Management Server with GuiDBedit Tool.
2. In the upper left pane, go to ***Table*** - ***Other*** - ***rad_services***.
3. In the upper right pane, select ***urlf_rad_service_0***.
4. In the lower pane, look at the value of ***cache_max_hash_size***.

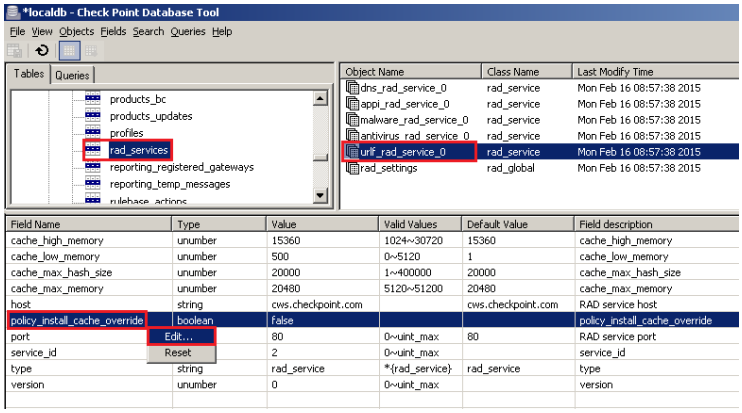


How to modify the limit of the URL Filtering cache?

1. Connect with SmartDashboard to Security Management Server / Domain Management Server.
2. Go to ***File*** menu - click on ***Database Revision Control...*** - create a revision snapshot.
3. Close all SmartConsole windows (SmartDashboard, SmartView Tracker, SmartView Monitor, etc.).
4. Connect with GuiDBedit Tool to Security Management Server / Domain Management Server.
5. In the upper left pane, go to ***Table*** - ***Other*** - ***rad_services***.
6. In the upper right pane, select ***urlf_rad_service_0***.
7. In the lower pane:
   A. Right-click on the ***cache_max_hash_size*** - select ***Edit...*** - set the desired limit **(in R75.46 and lower, value must NOT exceed 25000 !!! In R77.20 the limit is 400000!!)** - click on ***OK***:



   B. Right-click on the ***policy_install_cache_override*** - select ***Edit...*** - select "**true**" - click on ***OK***:



8. Save the changes: go to ***File*** menu - click on ***Save All***.

9. Close the GuiDBedit Tool.

10. Connect with SmartDashboard to Security Management Server / Domain Management Server.

11. Install the policy ***only*** on the involved Security Gateway / Cluster object.

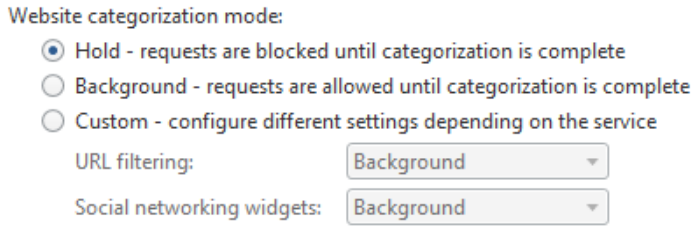
12. ***CRUCIAL STEP:*** Restore the default value for ***policy_install_cache_override*** ("false"):

Note: If default value ("false") is not restored, then URL Filtering kernel cache will be cleared on each policy installation.

For more examples consult sk90422

Timeout when using the function “hold connection”

There are 3 different behaviors that could be set on how a categorization will occur within a connection.



- **Background - connections are allowed until categorization is complete** - When a connection cannot be categorized with a cached response, an uncategorized response is received. The connection is allowed. In the background, the Check Point Online Web Service continues the categorization procedure. The response is cached locally for future requests (default). This option reduces latency in the categorization process.

- **Hold - connections are blocked until categorization is complete** - When a connection cannot be categorized with the cached responses, it remains blocked until the Check Point Online Web Service completes categorization.

- **Custom - configure different settings depending on the service** - Lets you set different modes for URL Filtering and Social networking widgets

The focus here will be on hold because by default the threshold before going into timeout is 4 seconds and therefore will not be suitable in a large environment. Sometime changing the default 4 seconds to a 10 seconds will change the users experience from a time out to a page that can load.

How to change the value of the timeout(don't survive reboot)

fw ctl set int psl_hold_trans_thresh 10

it can be reset to default with

fw ctl set int psl_hold_trans_thresh 4

To make it permanent it have to be add to fwkern.conf file
To change the kernel global parameters follow sk26202

UserCheck sessions

Problems could happen with block / Ask page when the amount of users rises as there are not enough HTTP sessions available on Security Gateway to host the portal pages.

Solution

1. Log into Expert mode
2. Edit the '/opt/CPUserCheckPortal/conf/php.ini' file in Vi editor

   [Expert@HostName]# vi /opt/CPUserCheckPortal/conf/php.ini
3. Decrease the value of 'session.gc_maxlifetime' parameter from 86400 to 1800:

   session.gc_maxlifetime=1800
4. Edit the '/opt/CPUserCheckPortal/conf/httpd.conf' file in Vi editor

   [Expert@HostName]# vi /opt/CPUserCheckPortal/conf/httpd.conf
   A. Increase the value of 'ServerLimit' parameter from 28 to 100:

      ServerLimit 100

      (sets the maximum configured value for MaxClients for the lifetime of the Apache process)

   B. Increase the value of 'MaxClients' parameter from 28 to 100:

      MaxClients 100

      (specifies the number of simultaneous requests that can be processed by Apache)

   C. Increase the value of 'MinSpareServers' parameter from 5 to 15:

      MinSpareServers 15

      (specifies the minimum number of idle child server processes for Apache, which is not handling a request)

   D. Increase the value of 'MaxSpareServers' parameter from 11 to 21:

      MaxSpareServers 21

      (specifies the maximum number of idle child server processes for Apache, which is not handling a request)

E. Set the value of 'StartServer' parameter to 5:

StartServers 5

(specifies the number of child server processes that will be created by Apache on start-up)

5. Restart the UserCheck Portal:

[Expert@HostName]# mpclient stop UserCheck
[Expert@HostName]# mpclient start UserCheck

Domain name object and FQDN

A Domain Object allows you to specify a domain name for matching in the rule base. It can be used in Source and Destination columns of Access Policy.

There are 2 modes in R80.10: FQDN mode and Non-FQDN mode.

Starting from R80.10, Domain objects do not disable SecureXL Accept templates anymore and support Templates Acceleration. Hence, Domain objects can be used in upper rules in the security policy with no performance impact.

However it is advice to not over use the domain object since they can cause latency due the many reverse lookup it had to do.

Ressources:

sk111303.
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111303&partition=General&product=All%22

sk97638
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638&partition=General&product=All%22#Related%20solutions

sk103422
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk103422&partition=Advanced&product=URL

sk90422
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk90422&partition=General&product=URL

sk26202
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk26202&partition=Advanced&product=Security

sk85040
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk85040&partition=Advanced&product=Security

