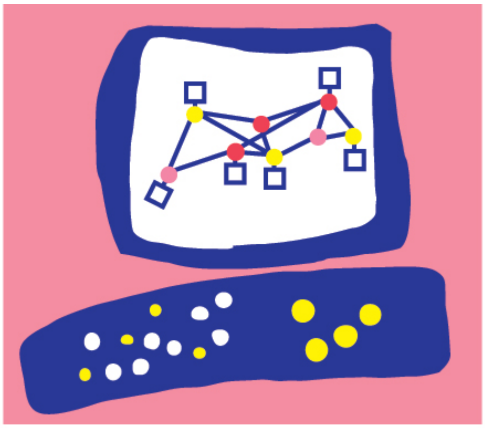
FQDN Objects: A Deeper Dive

2018 SE White papers

Adam Forester - SE Mid-South - TN - December 10, 2018



Check Point®

SOFTWARE TECHNOLOGIES LTD

Introduction

R80.10 now supports the usage of FQDN (fully qualified domain) objects within the firewall rulebase. These type of objects are a change from prior versions that only supported reverse lookup and were a critical performance impact. SK120633 describes usage in full detail. This document will be used to describe in more detail how FQDN objects are processed and how their performance can be tuned.

Basic Functionality

SK120633 describes two types of objects. FQDN and Non-FQDN. FQDN objects must be formatted with a preceding dot '.' (.checkpoint.com). Once installed the security gateway will do a forward lookup of the domain and cache the results. Both www.checkpoint.com and .checkpoint.com will be looked up and the results cache. The gateway will cache the results for 1 hour. FQDN objects do not support wildcards. Unlike previous versions the usage of FQDN objects does not disable acceleration.

Non-FQDN objects allow for the matching of up to 10 levels (a.b.c.d.e.f.g.h.i.j.checkpoint.com). By entering .checkpoint.com it would also match support.checkpoint.com. This functionality is done by using a reverse lookup. These objects can greatly affect a security gateways performance due to the reverse lookup, every packet that hits these rules has to be looked up. It is highly recommended to put these rules as low as possible if they MUST be used at all. In versions prior to R80.10 domain objects disabled acceleration, this is no longer the case in 80.10 and up.

Deeper Dive

Sk120633 does not describe the underlying function of the domain object and how it can affect the performance of a gateway. When a FQDN object, (.checkpoint.com), is created the gateway will begin doing a lookup of www.checkpoint.com & .checkpoint.com.

IN R80.10

Each FW_Worker process will lookup the 2 domains on each DNS Server that is configured. Consider a gateway with 8 fw_worker processes and 3 DNS servers configured.

That would be a total of 48 lookups per domain. (3 dns * 8 workers * 2 lookups (www & .)) This lookup happens every 30 seconds by default and IP results are cached for 1 hour.

IN R80.20

The lookup is only being performed by FW_Worker_0 this lookup happens every 60 seconds now, this has greatly reduced the lookup load on the gateway and streamlined the service.

HFA 142 and above should be the minimum version of 80.10 that domain objects are used on. HFA 142 resolved a lookup problem created by the use of FQDN objects. Versions prior to HFA 142 caused performance issues due to how lookups were handled. Prior to 142 all domain lookups would happen at the same time, using the math above (for 80.10) if we had 50 domain objects it would be 2400 dns queries every 30 seconds. After 142 queries are done in bunches. The total queries is the same but it is better distributed rather than being all at once. In 80.20 the lookups are even further reduced by FW_Worker_0 being the only process that executes queries.

CNAME support. Some domains do not point directly to an A record but instead can use a series of CNAME (canonical name) records to get to the resulting IP record. FQDN objects will resolve the CNAME records until an IP is cached.

Troubleshooting

The cache can be reviewed using fw tab commands.

- fw tab -t dns_reverse_cache_tbl -u -f **(80.10)**
- fw ctl multik print_bl dns_reverse_cache_tbl **(80.20)**
    - this will display the cache table for domain objects.
    - Key: is a hexadecimal version of the IP address
        - you can convert it using https://www.browserling.com/tools/hex-to-ip
    - If you just want the KEY in a list format you can run:

        - fw tab -t dns_reverse_cache_tbl -u |cut -f1 --d ";"|sort |uniq
- fw tab -t dns_reverse_unmatched_cache -u -f **(80.10)**
- fw ctl multik print_bl dns_reverse_unmatched_cache **(80.20)**
    - Shows unmatched IP addresses
    - Only used if non-FQDN objects are used.

As previously discussed non-FQDN objects can cause major performance impacts. Using the R80 API we can quickly confirm if a domain object is setup not as FQDN.

- mgmt_cli -r true show objects type "dns-domain" details-level full limit 500 --format json | jq --raw-output '.objects[] | .name + " " + (.”is-sub-domain"|tostring)'
    - this will output a list of all domain objects. If it says FALSE then it is FQDN, if it is TRUE then that object is a non-FQDN object.

- mgmt_cli -r true show objects type "dns-domain" details-level full limit 500 --format json | jq --raw-output '.objects[] | select(."is-sub-domain" == true) | .name’
    - This command will only output any objects that have been created that are non-FQDN objects.