

# SSL Offloading with Magento 2



Meet Magento™

SSL vs TLS  
SSL is the standard security protocol used to establish secure connections between a web server and a browser. TLS is the successor to SSL, providing improved security and compatibility.

#MM17DE

# **SSL vs TLS**

TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are protocols that provide data encryption and authentication between applications and servers

<https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html>

# 3 components (ssl proxy - varnish - magento 2)

multiple proxy options {  
Haproxy,  
NGINX,  
Google Cloud Load Balancing with SSL,  
Amazon EC2,  
Fastly,  
Section.io  
CloudFlare,  
Traefik,  
etc....  
}

# WHY NO SSL with Varnish

First, I have yet to see a SSL library  
where the source code is not a nightmare.

Second, it is not exactly the  
best source-code in the world.  
Even if I have no idea what it does,  
there are many aspect of it that scares me.



<https://www.varnish-cache.org/docs/trunk/phk/ssl.html#phk-ssl>

# Varnish 5

## Very Experimental HTTP/2 support

We are in the process of adding HTTP/2 support to Varnish, but the code is very green still - life happened.

But you can actually get a bit of traffic though it already, and we hope to have it production ready for the next major release ([2017-03-15](#)).

Varnish supports HTTP/1 -> 2 upgrade. For political reasons, no browsers support that, but tools like curl does.

For encrypted HTTP/2 traffic, put a [SSL proxy in front of Varnish](#).

HTTP/2 support is disabled by default, to enable, set the [http2](#) feature bit.

3 components (al proxy - varnish - magento 2)  
rulefile: prop\_stacks {  
 maxConnections;  
 maxRate;  
 Connection\_Credit\_Limit\_Balancing\_with\_SSL;  
 Allowance\_Rate;  
 Rate\_Limit;  
 Session\_Hash;  
 Connection\_Balance;  
 Transport;  
};

The diagram illustrates a network architecture. At the top center is a white cube labeled "3 components (al proxy - varnish - magento 2)" with a small red square at its base. Below it is a vertical stack of three white cubes. To the left of this stack is a large blue star shape. To the right is a blue arrow pointing upwards. The background consists of several other white cubes of varying sizes, some partially visible.

# Hardware vs Software

DO I NEED SSL certificate FOR EACH SERVER?



*If you do your load balancing on TCP or IP layer (OSI layer 4/3, a.k.a L4, L3), then yes, all HTTP servers will need to have the SSL certificate installed.*

*If you load balance on the HTTPS layer (L7), then you'd only install the certificate on the load balancer alone, and use plain un-encrypted HTTP over the local network between the load balancer and the web servers (for best performance on the web servers).*

# Hardware vs Software



## DO I NEED SSL certificate FOR EACH SERVER?

*If you do your load balancing on TCP or IP layer (OSI layer 4/3, a.k.a L4, L3), then yes, all HTTP servers will need to have the SSL certificate installed.*

*If you load balance on the HTTPS layer (L7), then you'd only install the certificate on the load balancer alone, and use plain un-encrypted HTTP over the local network between the load balancer and the webservers (for best performance on the web servers).*

*If you have a large installation, then you may be doing; Internet -> L3 load balancing -> layer of L7 SSL concentrators -> load balancers -> layer of L7 HTTP application servers...*



## Hardware vs Software

DO I NEED SSL certificate FOR EACH SERVER?

If you do your load balancing on TCP or IP layer (OSI layer 4/5), like L4, L5, then yes, all HTTP servers will need to have the SSL certificate installed.

If you load balance on the HTTPS layer (L7), then you'd only install the certificate on the load balancer alone, and use plain un-encrypted HTTP over the local network between the load balancer and the web servers (for best performance on the web servers).

If you have a large installation, then you may be doing Internet -> L3 load balancing -> layer of L7 SSL concentrators -> load balancers -> layer of L7 HTTP application servers...



**NGINX**  
CREATE ENDLESS COMBINATIONS...  
- Reverse proxy  
- Load Balancer  
- Web server  
- Application Accelerator  
- SSL offloading  
- Content delivery  
- Edge side includes  
- Dynamic content generation



128.1.1.94

TOUCH TO GO

The complete Internet  
experience. From static sites  
to the complex dynamic  
sites of today, Traefik  
lets you easily manage them  
all. It's fast, reliable, and  
secure.



traefik

## FASTLY VARNISH IN THE CLOUD

- Pre-configured Apache or Nginx setup  
- Pre-configured Magento 2 setup  
ONLY step to do is creating Fastly account and start tuning setup  
INSTALL: <https://github.com/fastly/fastly-magento2>



https://www.fastly.com/docs/api/2.0/using-the-control-panel/working-with-objects

## CLOUDFLARE

SIMPLE STEPS TO MAKE IT BETTER



DO IT! Step to do is SSL offloading



## LET'S ENCRYPT

BACK TO THE BASICS OF FREE SSL

- Pre-configured Apache setup  
- Pre-configured Apache for NGINX setup  
- Pre-configured Magento 2 setup  
- Let's Encrypt client (CERTBOT) (<https://letsencrypt.org/docs/certbot/>)

# SSL & Google 2017

MOVING TOWARDS A MORE SECURE WEB

*'Beginning in January 2017 (Chrome 56), we'll mark HTTP pages that collect passwords or credit cards as non-secure, as part of a long-term plan to mark all HTTP sites as non-secure.'*

25/08/17

Treatment of HTTP pages with password or credit card form fields:

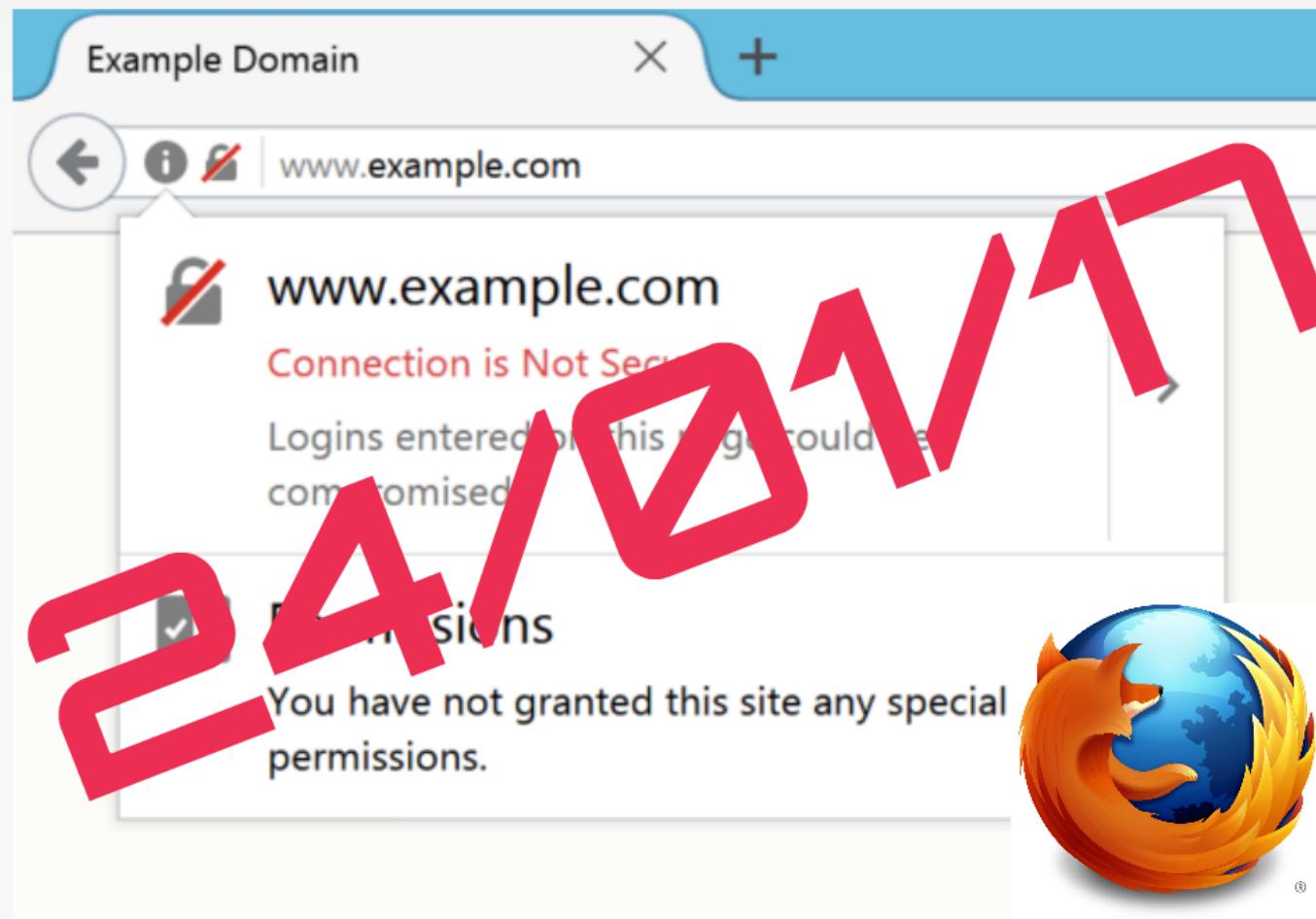
Current (Chrome 53)	Jan. 2017 (Chrome 56)
login.example.com	Not secure   login.example.com

<https://developers.google.com/web/updates/2017/01/nic56>  
[https://en.wikipedia.org/wiki/Google\\_Chrome\\_version\\_history](https://en.wikipedia.org/wiki/Google_Chrome_version_history)

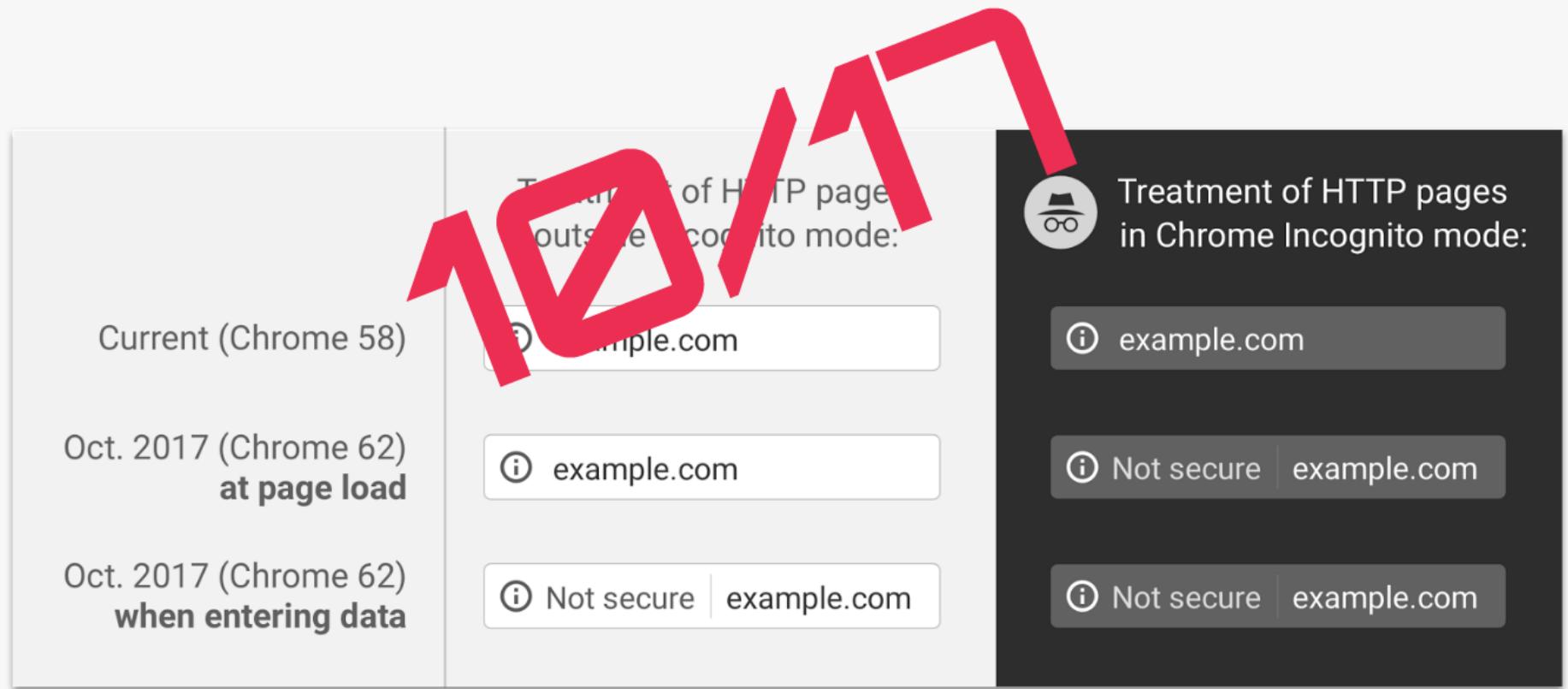
Firefox



# Firefox 51



# Chrome 62



Since the change in [Chrome 56](#), there has been a [23%](#) reduction in the fraction of navigations to HTTP pages with password or credit card forms.

<https://security.googleblog.com/2017/04/next-steps-toward-more-connection.html>

# Certificate Transparency

Google's Certificate Transparency project fixes several structural flaws in the SSL certificates system, which is the main cryptographic system that underlies all HTTPS connections.

These flaws weaken the reliability and effectiveness of encrypted Internet connections and can compromise critical TLS/SSL mechanisms, including domain validation, end-to-end encryption, and the chains of trust set up by certificate authorities.

If left unchecked, these flaws can facilitate a wide range of security attacks, such as website spoofing, server impersonation, and man-in-the-middle attacks.

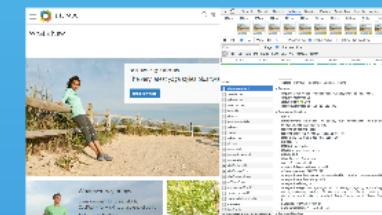
<https://www.certificate-transparency.org/>

# CLOUDFLARE

## SIMPLE STEPS TO MAX RESULT

- Pre-configured Varnish setup
- Pre-configured Apache or NGINX setup
- Pre-configured Magento 2 setup

*ONLY step to do is SSL offloading (incl HTTP/2)*



## Flexible SSL



## Full SSL

Requires SSL on your host



## Full SSL (strict)

Requires a valid SSL certificate



Visitor

CloudFlare

Origin server

## Full SSL (strict)

Requires a valid SSL certificate



### CNAME record

www

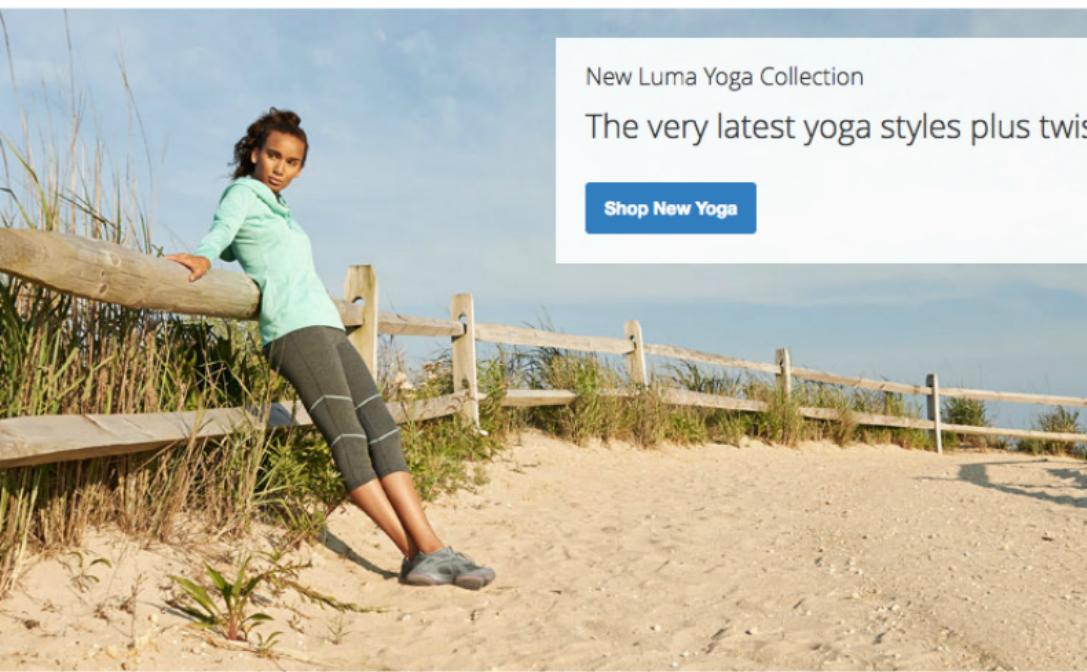
is an alias of supportdesk.shop

ttl Automatic





## What's New



New Luma Yoga Collection

The very latest yoga styles plus twists

[Shop New Yoga](#)



Whatever day brings

Luma Cocona™ for breathability,  
CoolTech™ for wicking, or a blend of both.

[Performance Fabrics >](#)



Network Timeline Profiles Application Security Audits

423 ms 558 ms 611 ms 652 ms 691 ms 753 ms 781 ms 793 ms 880 ms 1.05 s 1.18 s 1.38 s

Filter  Regex  Hide data URLs

All XHR JS CSS Img Media Font Doc WS Manifest Other

500 ms 1000 ms 1500 ms 2000 ms 2500 ms 3000 ms 3500 ms 4000 ms

Name	Headers	Preview	Response	Cookies	Timing
what-is-new.html	<input checked="" type="checkbox"/>				
calendar.css	<input type="checkbox"/>				
styles-m.css	<input type="checkbox"/>				
swatches.css	<input type="checkbox"/>				
require.js	<input type="checkbox"/>				
mixins.js	<input type="checkbox"/>				
requirejs-config.js	<input type="checkbox"/>				
styles.css	<input type="checkbox"/>				
logo.svg	<input type="checkbox"/>				
styles-l.css	<input type="checkbox"/>				
print.css	<input type="checkbox"/>				
new-main.jpg	<input type="checkbox"/>				
new-performance.jpg	<input type="checkbox"/>				
new-eco.jpg	<input type="checkbox"/>				
mb05-black-0.jpg	<input type="checkbox"/>				
mb06-gray-0.jpg	<input type="checkbox"/>				
wb07-brown-0.jpg	<input type="checkbox"/>				
ug05-gr-0.jpg	<input type="checkbox"/>				
opensans-400.woff2	<input type="checkbox"/>				
Luma-Icons.woff2	<input type="checkbox"/>				
jquery.mobile.custom.js	<input type="checkbox"/>				
responsive.js	<input type="checkbox"/>				
dataPost.js	<input type="checkbox"/>				

162 requests | 993 KB transferred..

General

Request URL: <https://supportdesk.shop/what-is-new.html>  
Request Method: GET  
Status Code: 200  
Remote Address: 104.28.11.100:443

Response Headers

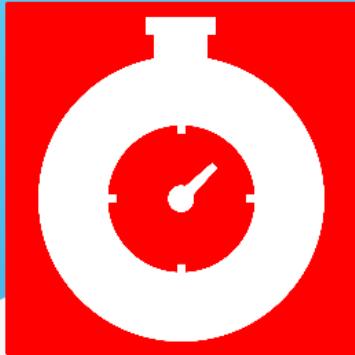
age: 6  
cache-control: no-store, no-cache, must-revalidate, max-age=0  
cf-ray: 2f29ddc63cd214b5-AMS  
content-encoding: gzip  
content-type: text/html; charset=UTF-8  
date: Sun, 16 Oct 2016 07:41:04 GMT  
expires: -1  
pragma: no-cache  
server: cloudflare-nginx  
status: 200  
vary: Accept-Encoding  
via: 1.1 varnish-v4  
x-content-type-options: nosniff  
x-frame-options: SAMEORIGIN  
x-magento-cache-control: max-age=86400, public, s-maxage=86400  
x-magento-cache-debug: HIT  
x-magento-debug: 1  
x-magento-tags: store,cms\_block,catalog\_category\_39,catalog\_category\_catalog\_category\_product\_39,store\_group,cms\_block\_,catalog\_product\_4\_catalog\_product,catalog\_product\_5,catalog\_product\_13,catalog\_product\_19  
x-varnish: 294968 3702988  
x-xss-protection: 1; mode=block

Request Headers

**expires:** -1  
**pragma:** no-cache  
**server:** cloudflare-nginx  
**status:** 200  
**vary:** Accept-Encoding  
**via:** 1.1 varnish-v4  
**x-content-type-options:** nosniff  
**x-frame-options:** SAMEORIGIN  
**x-magento-cache-control:** max-age=86400, public, s-maxage=86400  
**x-magento-cache-debug:** HIT  
**x-magento-debug:** 1  
**x-magento-tags:** store,cms\_block,catalog\_category\_39,catalog\_product\_39,store\_group,cms\_block\_,catalog\_product,catalog\_product\_5,catalog\_product\_13,catalog\_product\_9  
**x-varnish:** 294968 3702988  
**x-xss-protection:** 1; mode=block

# FASTLY

## VARNISH IN THE CLOUD

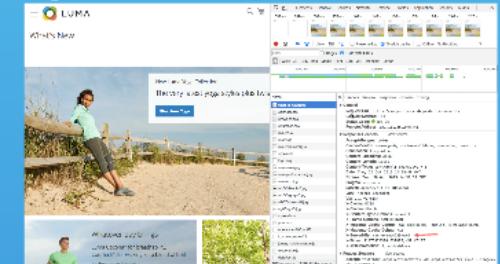


- Pre-configured Apache or NGINX setup
- Pre-configured Magento 2 setup

*ONLY step to do is creating Fastly account and start tuning setup  
CNAME DNS update to global.prod.fastly.net  
INSTALL <https://github.com/fastly/fastly-magento2>*

- Shared Domain Service \$0
  - Shared Certificate Service \$100
  - Shared Wildcard Certificate Service \$275
  - Customer Certificate Hosting Service \$???
- NO HTTP/2 :(

[<https://example.global.ssl.fastly.net/>]

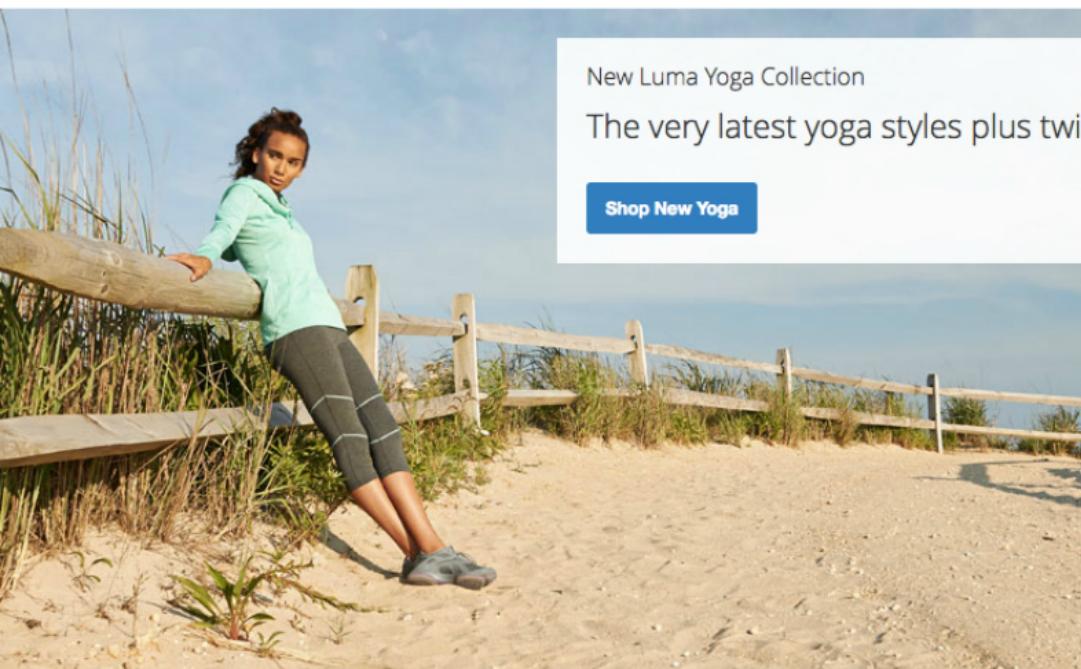


<https://docs.fastly.com/guides/securing-communications/ordering-a-paid-tls-option.html>

# e.global.ssl.fastly.net/]



## What's New



New Luma Yoga Collection

The very latest yoga styles plus twists

[Shop New Yoga](#)



Whatever day brings

Luma Cocona™ for breathability,  
CoolTech™ for wicking, or a blend of both.

[Performance Fabrics >](#)



Screenshot of the Network tab in a browser developer tools interface, showing network requests for the page. A red arrow points to the 'X-Served-By' header in the Response Headers section.

Network tab details:

- Request URL: <https://supportdesk.shop/what-is-new.html>
- Request Method: GET
- Status Code: 200 OK
- Remote Address: 151.101.36.249:443

Response Headers:

- Accept-Ranges: bytes
- Cache-Control: max-age=0, must-revalidate, no-cache, no-store
- Connection: keep-alive
- Content-Encoding: gzip
- Content-Length: 11189
- Content-Type: text/html; charset=UTF-8
- Date: Thu, 20 Oct 2016 14:38:48 GMT
- Expires: Tue, 20 Oct 2015 14:38:37 GMT
- Pragma: no-cache
- Server: Apache/2.4.18 (Ubuntu)
- Vary: Accept-Encoding
- Via: 1.1 varnish
- X-Cache: MISS
- X-Cache-Hits: 0
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- X-Magento-Cache-Control: max-age=86400, public, s-maxage=86400
- X-Magento-Cache-Debug: HIT
- X-Served-By: cache-ams4129-AMS
- X-Timer: S1476974328.631885,VS0,VE187
- X-XSS-Protection: 1; mode=block

Request Headers:

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Network timeline and resource list:

- what-is-new.html
- calendar.css
- styles-m.css
- swatches.css
- require.js
- mixins.js
- requirejs-config.js
- styles.css
- logo.svg
- new-main.jpg
- new-performance.jpg
- new-eco.jpg
- mb05-black-0.jpg
- mb06-gray-0.jpg
- wb07-brown-0.jpg
- ug05-gr-0.jpg
- styles-l.css
- print.css
- opensans-400.woff2
- Luma-Icons.woff2
- jquery.mobile.custom.js
- responsive.js
- dataPost.js

162 requests | 1007 KB transferred...

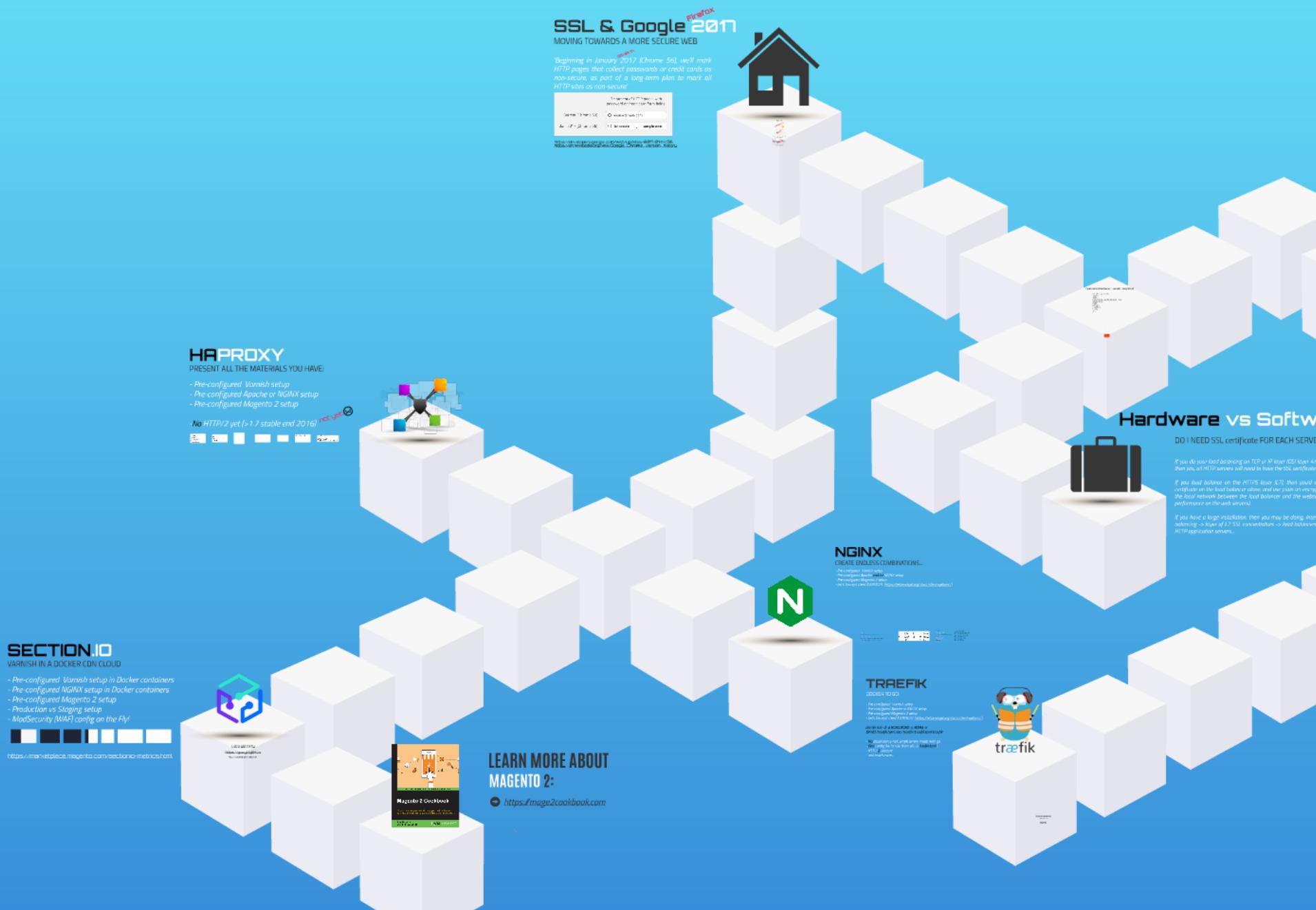
# Is-option.html

**Pragma:** no-cache  
**Server:** Apache/2.4.18 (Ubuntu)  
**Vary:** Accept-Encoding  
**Via:** 1.1 varnish  
**X-Cache:** MISS  
**X-Cache-Hits:** 0  
**X-Content-Type-Options:** nosniff  
**X-Frame-Options:** SAMEORIGIN  
**X-Magento-Cache-Control:** max-age=86400, public, s-maxage=86400  
**X-Magento-Cache-Debug:** HIT  
**X-Served-By:** cache-ams4129-AMS   
**X-Timer:** S1476974328.631885,VS0,VE187  
**X-XSS-Protection:** 1; mode=block

---

▼ Request Headers [view source](#)

**Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/\*,\*/\*;q=0.8



# NGINX

## CREATE ENDLESS COMBINATIONS...

- Pre-configured Varnish setup
- Pre-configured Apache and/or NGINX setup
- Pre-configured Magento 2 setup
- Let's Encrypt client (CERTBOT) [<https://letsencrypt.org/docs/client-options/>]



nginx/1.14.2  
Written by Igor Sysoev  
http://nginx.org  
http://nginx.org/en/docs/

nginx/1.14.2  
Written by Igor Sysoev  
http://nginx.org  
http://nginx.org/en/docs/

nginx/1.14.2  
Written by Igor Sysoev  
http://nginx.org  
http://nginx.org/en/docs/

```
location ~ \.php$ {
    # Pass the request on to Varnish.
    proxy_pass http://127.0.0.1:6081;

    # Pass a bunch of headers to the downstream server, so they'll know what's going on.
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

    # Most web apps can be configured to read this header and understand that the current session is actually HTTPS.
    proxy_set_header X-Forwarded-Proto https;

    # We expect the downstream servers to redirect to the right hostname, so don't do any rewrites here.
    proxy_redirect off;
}
```

```
root@supportdesk:/etc/nginx/conf.d# netstat -tulpn
```

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN	7514/nginx -g daemon
tcp	0	0	0.0.0.0:6081	0.0.0.0:*	LISTEN	7822/varnishd
tcp	0	0	127.0.0.1:6082	0.0.0.0:*	LISTEN	7822/varnishd
tcp	0	0	127.0.0.1:9001	0.0.0.0:*	LISTEN	2727/php-fpm.conf)
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	1297/mysqld
tcp	0	0	0.0.0.0:8080	0.0.0.0:*	LISTEN	7514/nginx -g daemon
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	7514/nginx -g daemon
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	1382/sshd
tcp6	0	0	:::6081	:::*	LISTEN	7822/varnishd
tcp6	0	0	:::22	:::*	LISTEN	1382/sshd

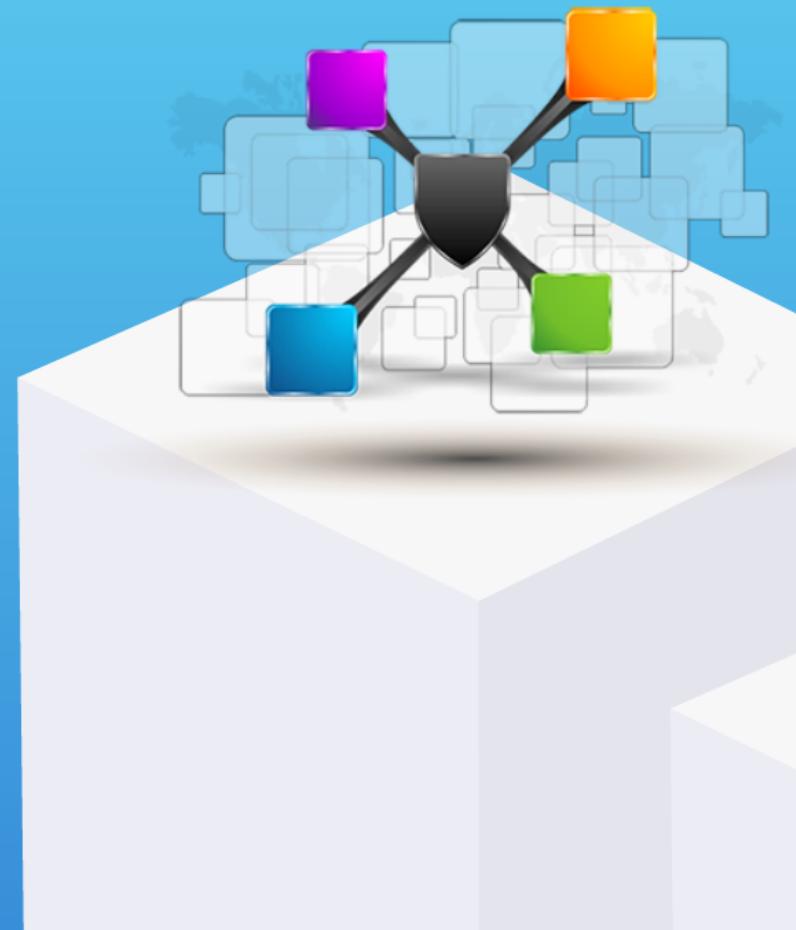
```
curl -I https://example.com/
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Oct 2016 18:03:00 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Magento-Cache-Control: max-age=86400, public, s-maxage=86400
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Thu, 22 Oct 2015 17:56:02 GMT
X-Magento-Cache-Debug: HIT
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
X-Varnish: 65607
Via: 1.1 varnish-v4
Accept-Ranges: bytes
```

```
/etc/varnish/default.vcl
#unset resp.http.X-Magento-Debug;
#unset resp.http.X-Magento-Tags;
#unset resp.http.X-Powered-By;
#unset resp.http.Server;
#unset resp.http.X-Varnish;
#unset resp.http.Via;
#unset resp.http.Link;
```

# Haproxy

PRESENT ALL THE MATERIALS YOU HAVE:

- *Pre-configured Varnish setup*
- *Pre-configured Apache or NGINX setup*
- *Pre-configured Magento 2 setup*
- *No HTTP/2 yet (>1.7 stable end 2016)* *not yet!* ☹



```
frontend http-in
    bind 82.196.4.34:80
    bind 82.196.4.34:443 ssl crt /etc/ssl/private/jira.nl.pem
    mode http
    option httpclose
    option http-server-close
    option forwardfor
    default_backend servers

backend servers
    reqadd X-Forwarded-Proto:\ https
    mode http
    balance leastconn
    cookie SERVERID insert indirect nocache
    redirect scheme https if !{ ssl_fc }
    server server1 82.196.4.104:6083 check send-proxy-v2
#server s1 82.196.5.10:80 check cookie s1 weight 1 maxqueue 25 rise 2 fall 1 maxconn 250

frontend http-in-proxy
    bind *:81
    default_backend servers-proxy

backend servers-proxy
    server server1-proxy 82.196.4.104:6083 send-proxy-v2
```

```
# edit that file.

# Should we start varnishd at boot? Set to "no" to disable.
START=yes

# Maximum number of open files (for ulimit -n)
NFILES=131072

# Maximum locked memory size (for ulimit -l)
# Used for locking the shared memory log in memory. If you increase log size,
# you need to increase this number as well
MEMLOCK=82000

DAEMON_OPTS="-a :6081 \
             -a :6083,PROXY \
             -T localhost:6082 \
             -f /etc/varnish/default.vcl \
             -S /etc/varnish/secret \
             -s malloc,256m"
```

```
vcl 4.0;

backend default {
    .host = "82.196.5.10";
    .port = "80";
}

acl purge {
    "localhost";
}

sub vcl_recv {
    set req.http.x-clientip = client.ip;
    set req.http.x-serverip = server.ip;
    set req.http.x-localip = local.ip;
    set req.http.x-remoteip = remote.ip;
    return(pass);

    if (req.method == "PURGE") {
        if (client.ip !~ purge) {
            return (synth(405, "Method not allowed"));
        }
        if (!req.http.X-Magento-Tags-Pattern) {
            return (synth(400, "X-Magento-Tags-Pattern header required"));
        }
        ban("obj.http.X-Magento-Tags ~ " + req.http.X-Magento-Tags-Pattern);
        return (synth(200, "Purged"));
    }

    if (req.method != "GET" &&
        req.method != "HEAD" &&
        req.method != "PUT" &&
        req.method != "POST" &&
        req.method != "TRACE" &&
        req.method != "OPTIONS" &&
        req.method != "DELETE") {
        /* Non-RFC2616 or CONNECT which is weird. */
        return (pipe);
    }

    # We only deal with GET and HEAD by default
    if (req.method != "GET" && req.method != "HEAD") {
        return (pass);
    }
}
```

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/magento

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory /var/www/html/magento>
        AllowOverride All
        Require all granted
    </Directory>

    SetEnv MAGE_MODE production
    #SetEnvIf X-Forwarded-Proto https HTTPS=on
    SetEnvIf X-Forwarded-Proto "^(https)" HTTPS=on
</VirtualHost>
```

~  
~  
~

1,1

All

## ⓘ Varnish Configuration

Access list

localhost

[GLOBAL]

IPs access list separated with \,\backslash that can purge Varnish configuration for config file generation. If field is empty default value localhost will be saved.

Backend host

82.196.4.104

[GLOBAL]

Specify backend host for config file generation. If field is empty default value localhost will be saved.

Backend port

6081

[GLOBAL]

Specify backend port for config file generation. If field is empty default value 8080 will be saved.

Export Configuration

Export VCL for Varnish 3

[GLOBAL]

Export VCL for Varnish 4

[GLOBAL]

```
<?php  
echo "Client IP: " . $_SERVER["HTTP_X_CLIENTIP"] . "<br />".PHP_EOL;  
echo "Server IP: " . $_SERVER["HTTP_X_SERVERIP"] . "<br />".PHP_EOL;  
echo "Local IP: " . $_SERVER["HTTP_X_LOCALIP"] . "<br />".PHP_EOL;  
echo "Remote IP: " . $_SERVER["HTTP_X_REMOTEIP"] . "<br />".PHP_EOL;  
echo "X-Forwarded-For: " . $_SERVER["HTTP_X_FORWARDED_FOR"] . "<br />".PHP_EOL;  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~
```

"proxy.php" 6L, 355C

1,1

All

Client IP: 72.213.70.220

Server IP: 82.196.4.34

Local IP: 82.196.4.104

Remote IP: 82.196.4.34

X-Forwarded-For: 72.213.70.220, 72.213.70.220

# SECTION.IO

VARNISH IN A DOCKER CDN CLOUD

- *Pre-configured Varnish setup in Docker containers*
- *Pre-configured NGINX setup in Docker containers*
- *Pre-configured Magento 2 setup*
- *Production vs Staging setup*
- *ModSecurity (WAF) config on the Fly!*



<https://marketplace.magento.com/sectionio-metrics.html>



Let's get Dirty

<https://goo.gl/gBYvu>

<https://gist.github.com/raybogman>

## My Stack

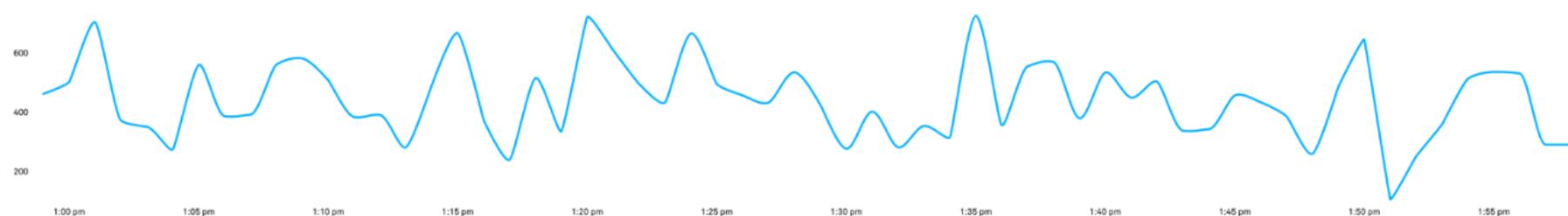


**Edge proxy**  
Protocol negotiation and routing. Handles SSL termination, HTTP/2 and more.

V Varnish Proxy  
S ModSecurity Proxy

E Edge Proxy  
O Origin Proxy

Number of HTTP responses served per minute



Response counts

Error responses

Response bandwidth

## Varnish

Cache hit, pass and misses for the last hour

Graph  
Relative

18.6%    16%    65.4%

Hit

Miss

Pass

?

How can we help?

54.252.190.175

# kibana

Discover Visualize Dashboard Settings

Last 15 minutes

Search...

account1-app1\*

Selected Fields

? \_source

Available Fields

? @timestamp

t @version

? XForwardedFor

t \_id

t \_index

t \_type

? accountid

? applicationid

? auditLogTrailer.Apache-Handler

? auditLogTrailer.Engine-Mode

? auditLogTrailer.Producer

? auditLogTrailer.Server

? auditLogTrailer.Stopwatch

? auditLogTrailer.Stopwatch2

? auditLogTrailer.WebApp-Info

? auditLogTrailer.messages

? audit\_logging\_time\_ms

? bytes

? combined\_processing\_time\_ms

t content\_type

? count

? environmentId

? garbage\_collection\_time\_ms

? geoip.area\_code

t geoip.city

? geoip.city\_name

? geoip.continent\_code

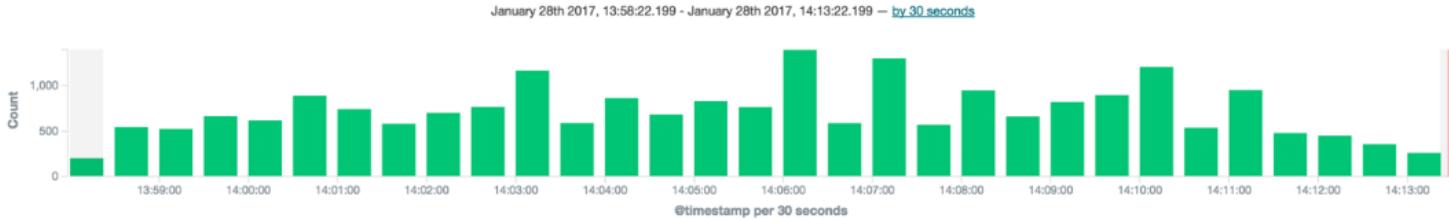
t geoip.country\_code2

? geoip.country\_code3

? geoip.country\_name

? geoip.dma\_code

? geoip.ip



Time ▾

\_source

▶ January 28th 2017, 14:13:12.000

```
sectionRegion: section_azure_australiaeast sectionNetwork: Managed Australia 4 scheme: http time_taken_ms: 3,342 useragent: Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) type: syslog ua.os: Other ua.name: Yahoo! Slurp ua.os_name: Other ua.device: Spider hostname: www.mouthsofmums.com.au instanceId: delivery-t5ichze34o5zw-gen9-3 environmentId: 1 uri_path: /about/ content_type: text/html @version: 1 section_io_id: 1761213495151711485609189.266 upstream_request_host: bootcamp.section.io remote_addr: 68.180.230.188 geoip.city: Sunnyvale geoip.country_code: US geoip.locations: -122.0074, 37.4249 tls_cipher: - verb: GET tags: beats_input_codec_plain_applied
```

▶ January 28th 2017, 14:13:11.000

```
@version: 1 @timestamp: January 28th 2017, 14:13:11.000 count: 1 environmentId: 1 instanceId: hosted proxyName: varnish accountId: 1 applicationId: 1 tags: beats_input_codec_plain_applied, access-log, varnish-ncsa-log, bootcamp-data bytes: 25,653 verb: GET uri_path: /about/ status: 200 referrer: http://<redacted> useragent: Mozilla/5.0 (Linux; Android 6.0.1; SM-G935F Build/MRM29K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/55.0.2883.91 Mobile Safari/537.36 [FB_IAB/FB4A;FBAV/108.0.0.17.68;] content_type: text/html time_taken_ms: 0.436 varnish handling: hit varnish hitmiss: hit section_io_id: 1761313495153611485609191.613 upstream_request_host: bootcamp.section.io
```

▶ January 28th 2017, 14:13:11.000

```
sectionRegion: section_azure_australiaeast sectionNetwork: Managed Australia 4 proxyName: last_proxy upstream_addr: 110.232.117.218 time_taken_ms: 11 http_x_forwarded_proto: http type: syslog upstream_status: 304 instanceId: hosted environmentId: 1 uri_path: /blog/ @version: 1 host: delivery-t5ichze34o5zw-gen9-2 section_io_id: - upstream_request_host: bootcamp.section.io upstream_header_time_seconds: 0.01 1 upstream_response_length: 0 verb: GET http_upgrade: - http_connection: - upstream_request_connection: upstream_http_cache_control: - tags: beats_input_codec_plain_applied, bootcamp-data accountId: 1 referrer: http://<redacted> @timestamp: January 28th 2017, 14:13:11.000
```

▶ January 28th 2017, 14:13:11.000

```
@version: 1 @timestamp: January 28th 2017, 14:13:11.000 instanceId: hosted sectionRegion: section_azure_australiaeast applicationId: 1 proxyName: last_proxy sectionNetwork: Managed Australia 4 environmentId: 1 accountId: 1 host: delivery-t5ichze34o5zw-gen9-2 tags: beats_input_codec_plain_applied, bootcamp-data http_x_forwarded_for: 68.180.230.188, 172.17.0.41 http_x_forwarded_proto: http http_upgrade: - http_connection: - status: 200 upstream_label: default upstream_status: 200 upstream_request_connection: upstream_request_host: bootcamp.section.io upstream_response_length: 13582 upstream_http_content_type: text/html upstream_http_cache_control: private bytes: 14,069
```

▶ January 28th 2017, 14:13:11.000

```
@version: 1 @timestamp: January 28th 2017, 14:13:11.000 instanceId: delivery-t5ichze34o5zw-gen9-2 sectionRegion: section_azure_australiaeast type: syslog sectionNetwork: Managed Australia 4 tags: beats_input_codec_plain_applied, routing, bootcamp-data region: section_azure_australia east accountId: 1 applicationId: 1 environmentId: 1 status: 200 time_taken_ms: 1,286 remote_addr: 68.180.230.188 hostname: www.mouthsofmums.com.au referrer: http://<redacted> useragent: Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) scheme: http tls_cipher: - tls_protocol: - bytes: 18,124 content_type: text/html section_io_id: 1761413495397011485609190.498 verb: GET uri_path: /about/
```

▶ January 28th 2017, 14:13:11.000

```
@version: 1 @timestamp: January 28th 2017, 14:13:11.000 sectionRegion: section_azure_australiaeast type: syslog sectionNetwork: Managed Australia 4 instanceId: delivery-t5ichze34o5zw-gen9-3 tags: beats_input_codec_plain_applied, routing, bootcamp-data region: section_azure_australiaeast
```



Dashboard



Stack



Overview



Diagnostics



Metrics



Alerting

Logs



Traces

Deployments

Configuration

Proxy

Repository

Domains

HTTPS

Split

API

Restrictions

State

Manage

Proxy ▾

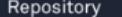
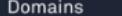
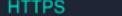
## Varnish Log

- From here you can find diagnostic information on the requests being handled by varnish. This is using the `varnishlog` tool. Click on the `Load` button to retrieve the last 500 lines of varnishlog from your delivery nodes.  
**Technical Note:** This will run `varnishlog -d` on the varnish containers in this environment.



## Results from varnishlog

```
19 SessionOpen  c 172.17.42.1 51915 :80
19 ReqStart    c 172.17.42.1 51915 742209755
19 RxRequest   c GET
19 RxURL      c /redacted
19 RxProtocol  c HTTP/1.1
19 RxHeader    c Host: bootcamp.section.io
19 RxHeader    c X-Forwarded-Proto: http
19 RxHeader    c X-Forwarded-For: 173.252.112.107
19 RxHeader    c section-io-id: 38807261307334411443750803.516
19 RxHeader    c User-Agent: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)
19 RxHeader    c Accept: */
19 RxHeader    c Accept-Encoding: deflate, gzip
19 VCL_call    c recv
19 VCL_Log     c req.xid:742209755
19 VCL_return  c lookup
19 VCL_call    c hash
19 Hash        c no_unique_cookie
19 Hash        c 635604354115400000
19 Hash        c http
19 Hash        c /redacted
19 Hash        c bootcamp.section.io
19 VCL_return  c hash
19 VCL_call    c miss fetch
19 Backend    c 16 default default
19 TTL         c 742209755 RFC 604800 -1 -1 1443750804 0 1443750803 1444355603 604800
19 VCL_call    c fetch
19 TTL         c 742209755 VCL 604800 86400 -1 1443750804 -0
19 VCL_Log     c backend=default
19 TTL         c 742209755 VCL 120 86400 -1 1443750804 -0
19 VCL_return  c hit_for_pass
19 ObjProtocol c HTTP/1.1
19 ObjResponse c OK
19 ObjHeader   c Date: Fri, 02 Oct 2015 01:53:23 GMT
19 ObjHeader   c Server: nginx
19 ObjHeader   c Content-Type: image/jpeg
19 ObjHeader   c Content-Length: 36831
19 ObjHeader   c Accept-Ranges: bytes
19 ObjHeader   c Cache-Control: max-age=604800
```

-  [Dashboard](#)
-  [Stack](#)
-  [Overview](#)
-  [Diagnostics](#)
-  [Metrics](#)
-  [Alerting](#)
-  [Logs](#)
-  [Traces](#)
-  [Deployments](#)
-  [Configuration](#)
-  [Proxy](#)
-  [Repository](#)
-  [Domains](#)
-  [HTTPS](#)
-  [Split](#)
-  [API](#)
-  [Restrictions](#)
-  [State](#)
-  [Manage](#)

## HTTPS

Your domain [bootcamp.section.io](#) is configured for HTTPS using a **custom certificate**.

Switching to [Let's Encrypt](#) provides you the freedom of not having to renew your certificates when they expire. Switching to Let's Encrypt is seamless.

[Change custom certificate](#)[Switch to Let's Encrypt](#)

### Certificate

Common name: \*.section.io

Alternate names: section.io

Issued by: DigiCert SHA2 Secure Server CA

Expiry: 2016-03-02T12:00:00.000Z

[HPKP fingerprint](#): KTUx4Xva/GeMQU9vR8LlzWox8ok8g9JJSZQhxAKxlo=

-  [Dashboard](#)
-  [Stack](#)
-  [Overview](#)
-  [Diagnostics](#)
-  [Metrics](#)
-  [Alerting](#)
-  [Logs](#)
-  [Traces](#)
-  [Deployments](#)
-  [Configuration](#)
-  [Proxy](#)
-  [Repository](#)
-  [Domains](#)
-  [HTTPS](#)
-  [Split](#)
-  [API](#)
-  [Restrictions](#)
-  [State](#)
-  [Manage](#)

- This action requires administrator privileges

Ask your account owner to perform this task, or to grant you the required access.

## Split bootcamp.section.io

This page enables you to create a new section.io application that will be responsible for handling requests for a subset of the URLs currently handled by the selected application.

Splitting the application will: [\(click for more\)](#)

After the split is complete, you can modify each application independently to achieve different proxy behaviour for each part of the URL space.

### This application

Current path prefix(es): /

### New application

Path Prefix:

/

Environment Name	Hosted	New URL Space
Production	Yes	http(s)://bootcamp.section.io/
Development	No	http(s)://bootcamp.section.io/

[Split](#)

# Varnish Cache for Magento

sectionio   

## SECTION.IO ACCOUNT SETTINGS

Account Credentials

Management

View Site Metrics

## Account and Application Selection

 Please choose your account and application. For questions or assistance, please [click here](#).

[Refresh Accounts and Applications](#)

Account 

Application 

[Update application](#)

## Management

Update Varnish Configuration with section.io. It will update and apply configuration in the **Production branch**.

[Update varnish configuration](#)

Complementary one click HTTPS certificate via LetsEncrypt. Domain **magento2.sectiondemo.com** must be exposed on the internet over port 80/HTTP.

[One click HTTPS](#)

# Varnish Cache for Magento

   sectionio 

## SECTION.IO ACCOUNT SETTINGS

Account Credentials

Management

**View Site Metrics**



Learn more about section.io. Get support from section.io.

### Overall Cache Hit Count

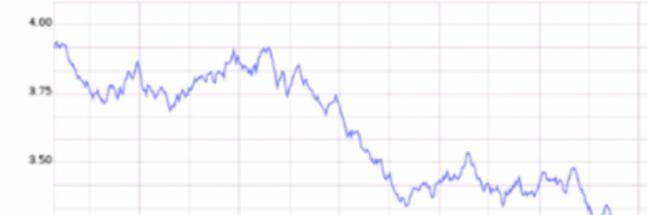
This chart shows how often your customer requests are able to be answered by the cache (a "cache hit"). The higher this rate, the faster your website loads and the less work required by your servers. You can increase this rate by caching more content. [Read more](#).



[View this in the section.io console.](#)

### HTML Cache Hit Count

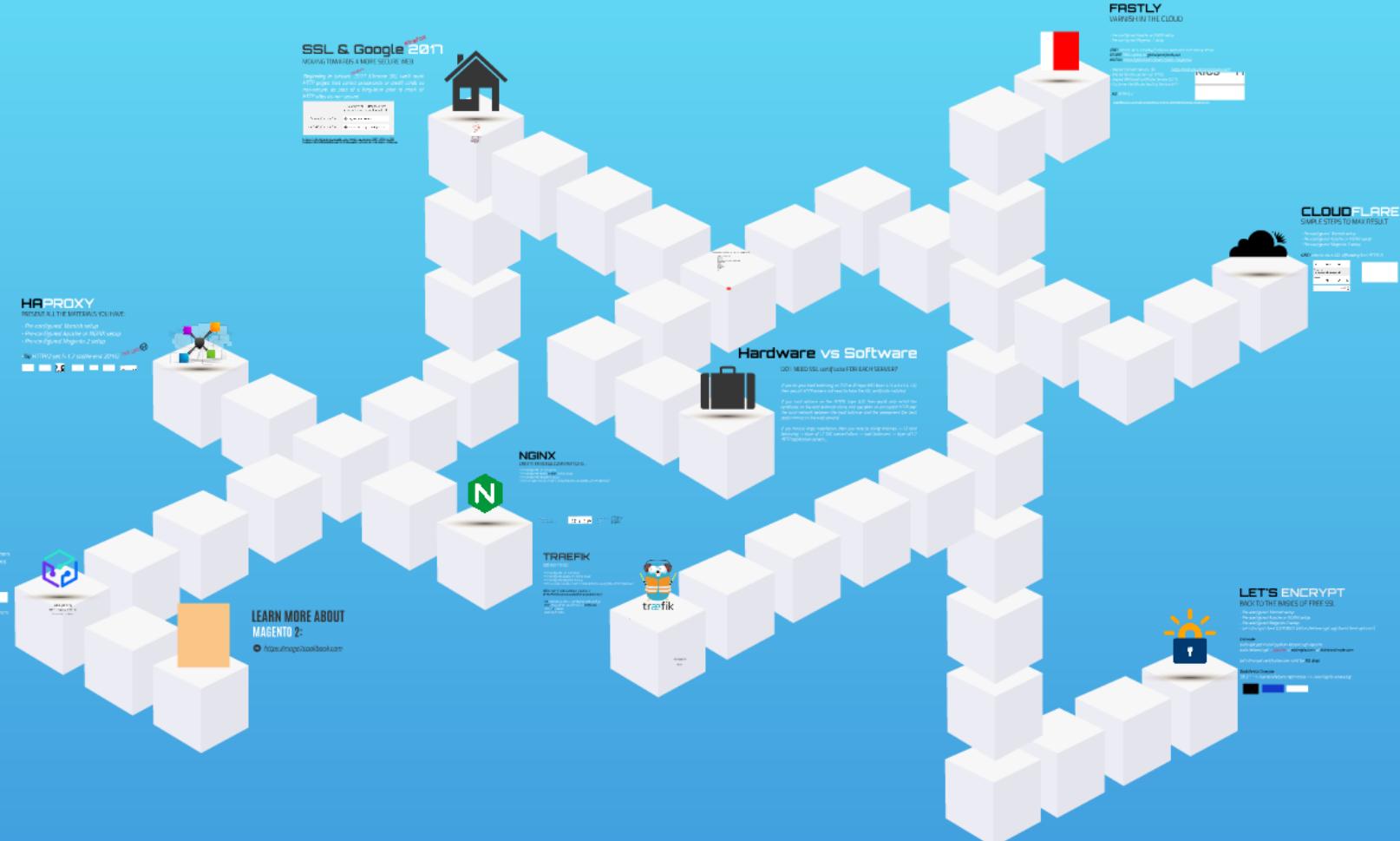
This chart shows how often your HTML document requests are able to be answered by the cache (a "cache hit"). HTML documents are a set of instructions used to create the web page. Magento generates these documents for you and they consume a significant amount of your server resources. Serving these documents from the cache instead of your server is a critical way to increase performance. [Read more](#).



# Let's get Dirty

<https://goo.gl/VgBYvU>

<https://gist.github.com/raybogman>



# LET'S ENCRYPT

## BACK TO THE BASICS OF FREE SSL



- Pre-configured Varnish setup
- Pre-configured Apache or NGINX setup
- Pre-configured Magento 2 setup
- Let's Encrypt client (CERTBOT) [<https://letsencrypt.org/docs/client-options/>]

*Example:*

```
sudo apt-get install python-letsencrypt-apache  
sudo letsencrypt --apache -d example.com -d www.example.com
```

*Let's Encrypt certificates are valid for 90 days*

*Update via Cronjob:*

```
30 2 * * 1 /usr/bin/letsencrypt renew >> /var/log/le-renew.log
```



Please choose whether HTTPS access is required or optional.

**Easy**

Allow both HTTP and HTTPS access to these sites

**Secure**

Make all requests redirect to secure HTTPS access

}

< OK >

<Cancel>

Congratulations! You have successfully enabled  
<https://supportdesk.shop>

You should test your configuration at:  
<https://www.ssllabs.com/ssltest/analyze.html?d=supportdesk.shop>

< **OK** >

- Congratulations! Your certificate and chain have been saved at /etc/letsencrypt/live/supportdesk.shop/fullchain.pem. Your cert will expire on 2017-01-17. To obtain a new version of the certificate in the future, simply run Let's Encrypt again.
- If you like Let's Encrypt, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>

Donating to EFF: <https://eff.org/donate-le>

## Hardware vs Software

### DO I NEED SSL certificate FOR EACH SERVER?



If you do your load balancing on TCP or IP layer (OSI layer 4/5), aka L4, L5R, then yes, all HTTP servers will need to have the SSL certificate installed.

If you load balance on the HTTPS layer (L7), then you'll only install the certificate on the load balancer alone, and use plain un-encrypted HTTP over the local network between the load balancer and the web servers (for best performance on the web servers).

If you have a large installation, then you may do: Internet -> L3 load balancing -> layer of L7 SSL concentrators -> load balancers -> layer of L7 HTTP application servers.

### NGINX

#### CREATE ENDLESS COMBINATIONS...

- Pre-configured Apache or Nginx setup
- Pre-configured MySQL or PostgreSQL
- Pre-configured PHP 5.6 setup
- Let's Encrypt client (SSL/TLS certificates)



### TRAEFIK

#### DOCKER TO GO

- Pre-configured Docker setup
- Pre-configured Apache or Nginx setup
- Pre-configured MySQL or PostgreSQL
- Let's Encrypt client (SSL/TLS certificates)

docker run -d -p 8000:8000 traefik --api --docker

Any container with single-layer mode set to true will be taken care of by Traefik.

and much more...



## LET'S ENCRYPT

### BACK TO THE BASICS

- Pre-configured Varnish setup
- Pre-configured Apache or Nginx setup
- Pre-configured MySQL 5.6 setup
- Let's Encrypt client (SSL/TLS certificates)

Example:  
sudo apt-get install python-letsencrypt  
sudo letsencrypt --register -d example.com

Let's Encrypt certificates are valid for 90 days.

Update via Cronjob:  
30 \* \* \* \* /usr/bin/letsencrypt renew



# TRAEFIK

## DOCKER TO GO

- Pre-configured Varnish setup
- Pre-configured Apache or NGINX setup
- Pre-configured Magento 2 setup
- Let's Encrypt client (CERTBOT) [<https://letsencrypt.org/docs/client-options/>]

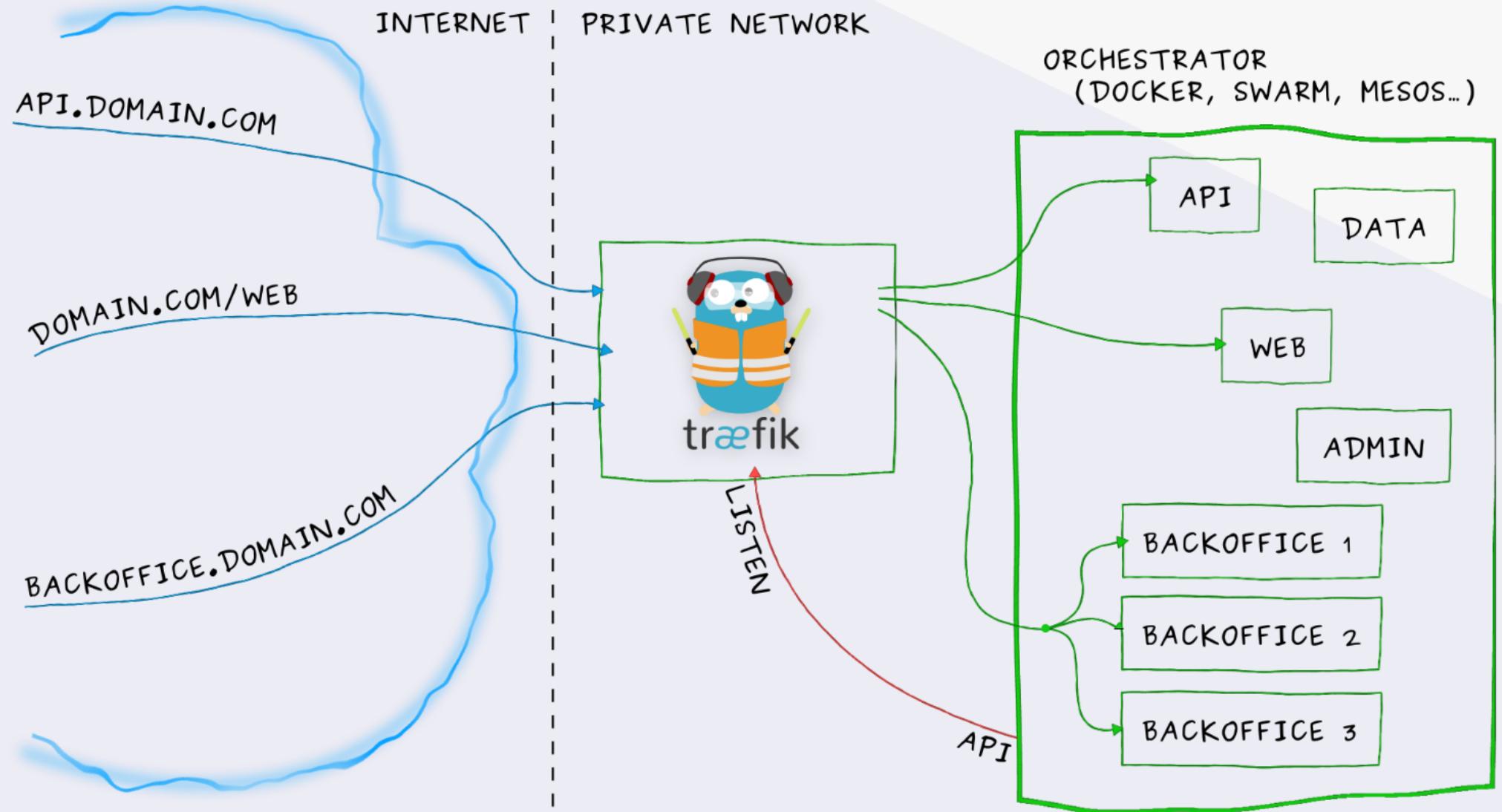
```
docker run -d -p 8080:8080 -p 80:80 -v  
$PWD/traefik.toml:/etc/traefik/traefik.toml traefik
```

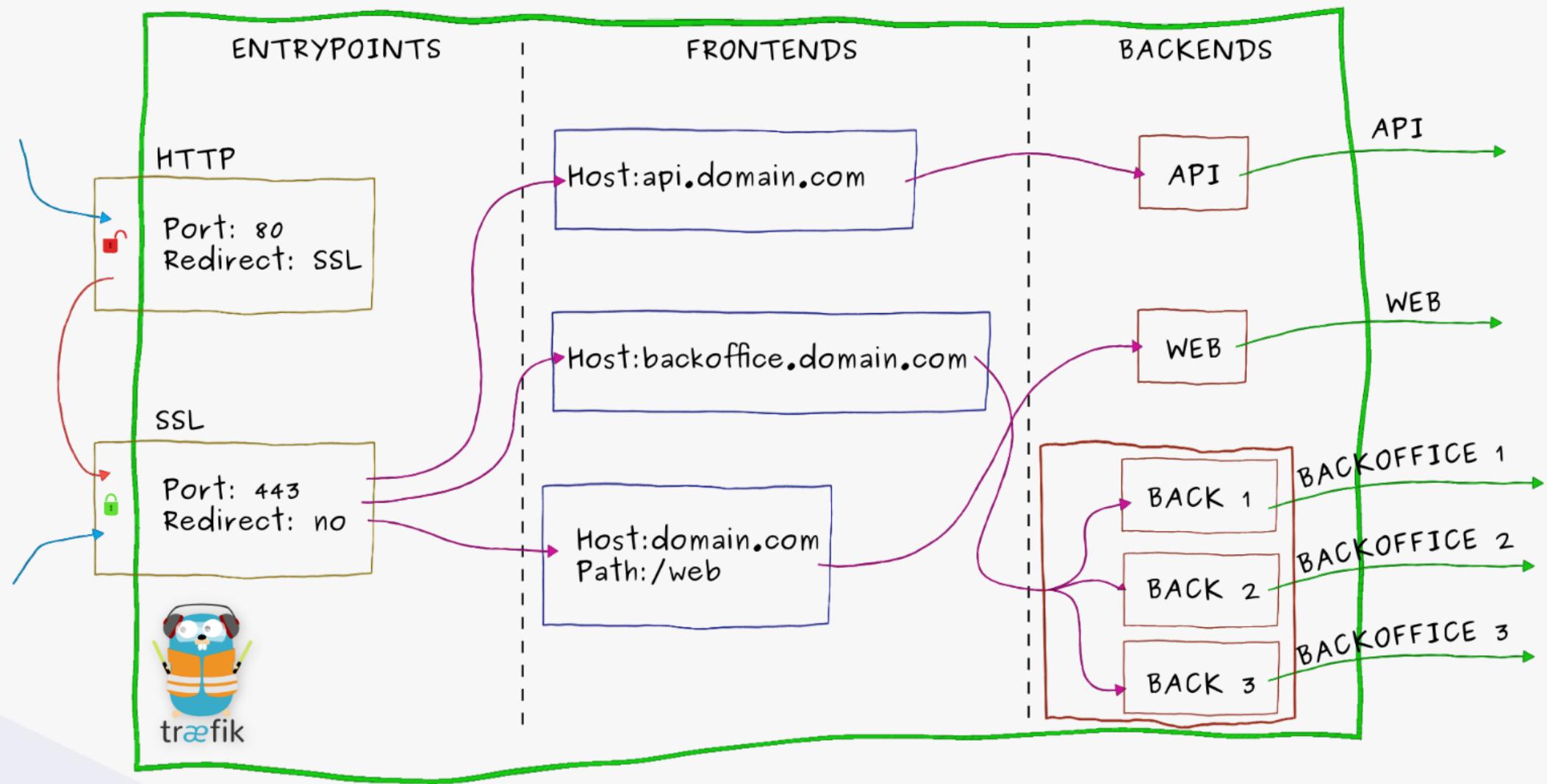
- No dependency hell, single binary made with go
- One config file to rule them all ;-)(traefik.toml)
- HTTP/2 support
- and much more...



traæfik



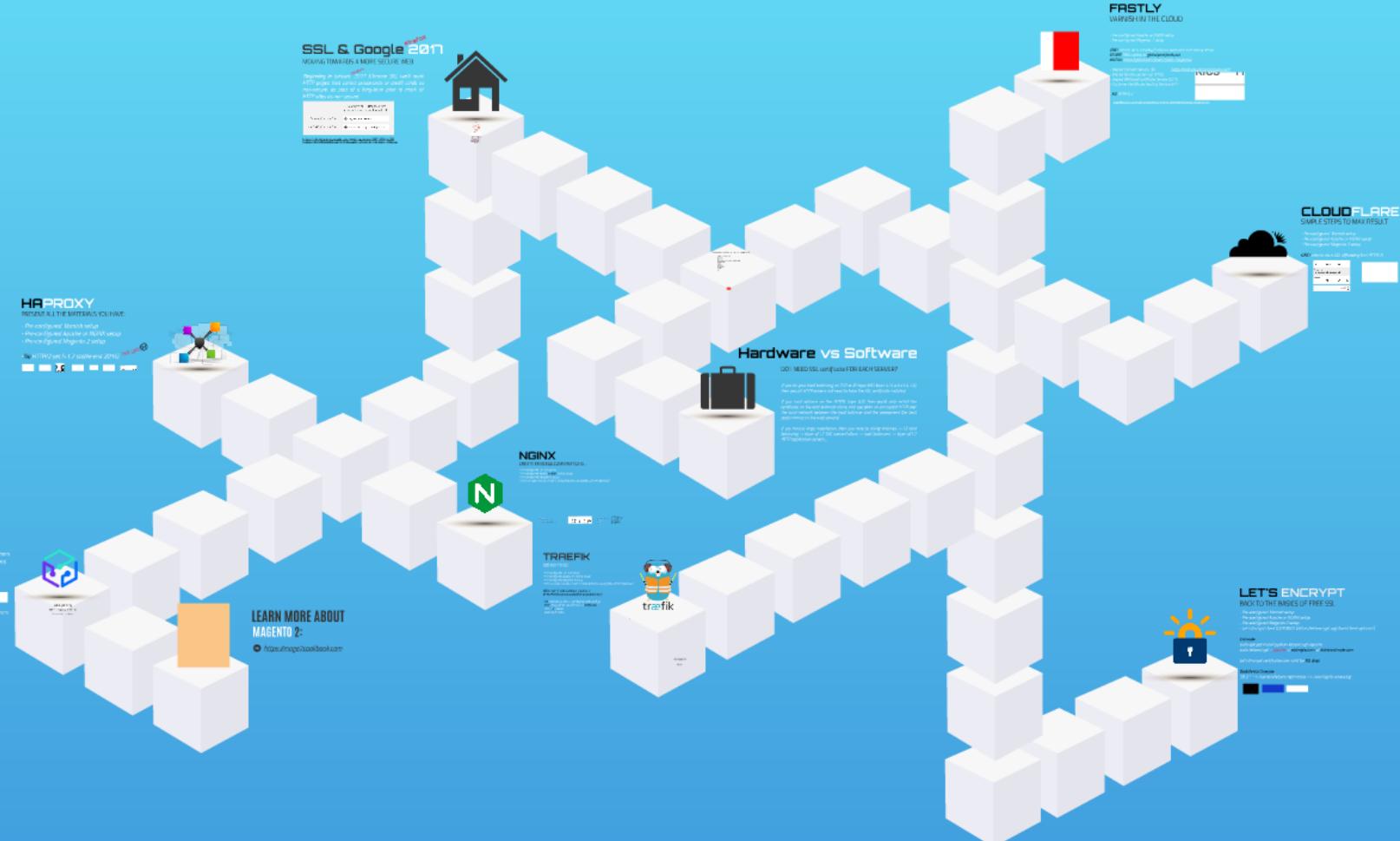




# **CONCLUSION**

**SSL TO GO or NOT TO GO**

**???????**





# LEARN MORE ABOUT MAGENTO 2:



<https://mage2cookbook.com>

# Creative Contributions by:

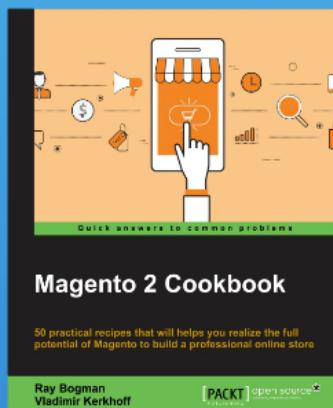


## Ray Bogman

- Magento Evangelist
- Trainer
- Performance nerd
- Security geek
- SEO freak



@raybogman  
@supportdesknu



<https://www.linkedin.com/in/raybogman>

The SupportDesk website homepage. It features a large orange "SupportDesk" logo with a plus sign icon. Below it, the text "Support voor Magento en Joomla!" is displayed. A cartoon character of a person in an orange jumpsuit and hard hat is holding a wrench. Two columns of services are listed with checkmarks: "Performance optimalisatie", "Theming, templating", "Maatwerk training", "SEO, SEM, SEA", "Consultancy", "Upgrade", "Migratie", "Security", "Hosting", "Mobile", and "APK". At the bottom, there is a call-to-action: "Meer weten? www.supportdesk.nu Of bel 020-337 5961". Logos for Magento and Joomla are also present.