

```

server {
    listen 80;
    listen [::]:80;
    listen 443 ssl http2;
    listen [::]:443 ssl;
    # include snippets/snakeoil.conf;
    keepalive_timeout 70;
    gzip off;

    root /var/www/html;

    # Add index.php to the list if you are using PHP
    index index.php index.html index.htm cdn.html cdn.php watch.html
    watch.php low.html low.php live.html live.php;

    server_name YOURSERVERNAMEHERE.xyz www.YOURSERVERNAMEHERE.xyz;

    ssl_certificate /etc/letsencrypt/live/YOURSERVERNAMEHERE.xyz/
    fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/YOURSERVERNAMEHERE.xyz/
    privkey.pem;
    ssl_trusted_certificate /etc/letsencrypt/live/
    YOURSERVERNAMEHERE.xyz/chain.pem;
    ssl_dhparam /etc/ssl/certs/dhparam.pem;

    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_session_cache shared:le_nginx_SSL:1m;
    ssl_session_timeout 1440m;
    ssl_prefer_server_ciphers on;
    ssl_session_tickets off;
    ssl_stapling off;
    ssl_stapling_verify on;
    resolver 8.8.8.8 8.8.4.4 valid=300s;
    resolver_timeout 5s;
    ssl_ecdh_curve secp384r1;

    ssl_ciphers
    "EECDH+AESGCM:EDH+AESGCM:ECDHE-RSA-AES128-GCM-SHA256:AES256+EECDH:DHE-
    RSA-AES128-GCM-SHA256:AES256+EDH:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-
    AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-
    SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-
    SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-
    SHA:ECHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES256-GCM-
    SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:AES256-
    SHA:AES128-SHA:DES-CBC3-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!
    PSK:!RC4";

    add_header Strict-Transport-Security "max-age=63072000;";
    add_header X-Frame-Options "DENY";

```

```

# Redirect non-https traffic to https
#   if ($scheme != "https") { return 301 https://
$host$request_uri;
#   }

location / {
    location ~* \.m3u8$ {
        add_header Cache-Control no-cache;
    }
    add_header Access-Control-Allow-Origin *;

# First attempt to serve file, then as directory, then a 404.
    try_files $uri $uri/ =404;
}

# pass PHP scripts to FastCGI server

location ~ /\.php$ {
    include snippets/fastcgi-php.conf;
# # With php-fpm (or other unix sockets):
    fastcgi_pass unix:/var/run/php/php7.2-fpm.sock;
# # With php-cgi (or other tcp sockets):
# fastcgi_pass 127.0.0.1:9000;
}

# deny access to .htaccess files, if Apache's document root
# concurs with nginx's one

#location ~ /\.ht {
#    deny all;
#}

# This provides RTMP statistics in XML at http://your-server-address/
# stat
location /stat {
    rtmp_stat all;
    rtmp_stat_stylesheet stat.xsl;
# auth_basic "Restricted Content";
#     # auth_basic_user_file /etc/nginx/.htpasswd;
}

# XML stylesheet to view RTMP stats. Copy stat.xsl wherever you want
# and put the full directory path here
location /stat.xsl {
    root /var/www/html/;
}

# Control interface (extremely useful, but can also boot people from
# streams so we put basic auth in front of it -
# see https://github.com/arut/nginx-rtmp-module/wiki/Control-module

```

for more info

```
#location /control {
    # you'll need a htpasswd auth file, that's outside the scope of
    this doc but any apache one will work
    #auth_basic "Restricted Content"; auth_basic_user_file /etc/
    nginx/.htpasswd; rtmp_control all;
    #}

#creates the http-location for our full-res desktop HLS stream
"http://my-ip/live/my-stream-key/index.m3u8"
location /live {
    # root /var/livestream/hls;
    alias /var/livestream/hls;
    expires -1;
    autoindex on;
    autoindex_localtime on;
    # CORS setup #
    set $sent_http_accept_ranges bytes;
    add_header 'Cache-Control' 'no-cache';
    add_header Cache-Control no-cache;
    add_header 'Access-Control-Allow-Origin' '*' always;
    add_header 'Access-Control-Expose-Headers' 'Content-Length';
    # allow CORS preflight requests #
    if ($request_method = 'OPTIONS') {
        add_header 'Access-Control-Allow-Origin' '*';
        add_header 'Access-Control-Max-Age' 1728000;
        add_header 'Content-Type' 'text/plain charset=UTF-8';
        add_header 'Content-Length' 0;
        return 204;
    }
    types {
        application/vnd.apple.mpegurl m3u8;
        application/dash+xml mpd;
        video/mp2t ts;
    }
}

#creates the http-location for our mobile-device HLS stream -
"http://my-ip/low/my-stream-key/index.m3u8"
location /low {
    # Disable cache
    add_header 'Cache-Control' 'no-cache';
    # CORS setup
    add_header 'Access-Control-Allow-Origin' '*'
always;
    add_header 'Access-Control-Expose-Headers'
'Content-Length';
    # allow CORS preflight requests
    if ($request_method = 'OPTIONS') {
        add_header 'Access-Control-Allow-Origin'
```

```

'*';
1728000;
charset=UTF-8';
        add_header 'Access-Control-Max-Age'
        add_header 'Content-Type' 'text/plain
        add_header 'Content-Length' 0;
        return 204;
    }
    types {
        application/vnd.apple.mpegurl m3u8;
    }
    alias /var/livestream/low;
}

#####enable nginx_status below#####
    location /nginx_status {
    # Enable Nginx stats
    stub_status on;
    # Only allow access from your IP e.g 1.1.1.1 or localhost OR ANYPLACE
YOU WANT TO BE ABLE TO SEE YOUR STATISTICS#
    allow YOUR.HOME.IP.ADDRESS; #PUT IN ANY IP ADDRESSES THAT YOU
WANT TO BE ABLE TO USE THIS SERVER FROM #####
    allow YOUR.CHURCH.IP.ADDRESS;
    allow 127.0.0.1;
    # Other request should be denied
    deny all;
    }

    location /live.html {
    root /var/www/html/;
    allow YOUR.HOME.IP.ADDRESS; #PUT IN ANY IP ADDRESSES THAT YOU
WANT TO BE ABLE TO USE THIS SERVER FROM #####
    allow YOUR.CHURCH.IP.ADDRESS;
    }

    location /low.html {
    root /var/www/html/;
    allow YOUR.HOME.IP.ADDRESS; #PUT IN ANY IP ADDRESSES THAT YOU
WANT TO BE ABLE TO USE THIS SERVER FROM #####
    allow YOUR.CHURCH.IP.ADDRESS;
    }
}

```