How to use IP Geolocation Regulatory Compliance Data Feeds with Nginx and Apache?

Posted on January 27, 2023

There are two common ways to configure deny lists for Nginx:

- With the use of the Nginx **include** module;
- With the use of the Nginx **geo** module.

1. How to use data feeds with the Nginx include module?

The required configuration file should be either placed in the already included '*nginx/conf.d*' folder or can be called directly by including it in the '*location*' directive. Which folders are included currently can be checked in *nginx.conf*:

```
include /etc/nginx/conf.d/*.conf;
```

Example of *./mySite.conf* if the deny list does not reside in the default config folder:

```
location / {
    include /etc/nginx/my_deny_nginx.conf;
    allow all;
    try_files $uri $uri @allowed;
    error_page 403 = @denied;
}
```

```
location @allowed {
    default_type text/html;
    return 200 'Your $REMOTE_ADDR is allowed';
}
location @denied {
    default_type text/html;
    return 403 'Your $REMOTE_ADDR is blocked';
}
```

Example of *my_deny_nginx.conf*:

```
deny 1.0.1.0/24;
deny 1.0.2.0/23;
deny 1.0.4.0/32;
deny 1.0.8.0/21;
deny 1.0.16.0/32;
deny 1.0.32.0/19;
deny 1.0.64.0/32;
```

Usage with rewrite module

Note that if you are using the Nginx's **rewrite** module, it precedes **include** directives. In this case, use **if** statements. Example of the config with **rewrite** module usage (302 redirects):

```
location / {
include /etc/nginx/my_deny_nginx.conf;
allow all;
try_files $uri $uri @allowed;
error_page 403 = @denied;
return 302 https://$new-site$request_uri;
}
```

To overcome this, a redirect can be used inside the **if** statement. For example, redirect HTTP to HTTPS:

Without **if** statement:

```
server_name mySite.localhost.local;
     location ~^/[^/]+$ {
             return     302 https://$server_name$request_uri;
     }
```

With **if** statement:

```
server_name mySite.localhost.local;
     location ~^/[^/]+$ {
             if ($host = 'http://mySite.localhost.local' ) {
                     rewrite  ^/(.*)$  https://mySite.localhost.local/$1;
             }
     }
```

How to convert the data feed to Nginx deny list?

To create *my_deny_nginx.conf*:

- Download the data feed in CIDR notation to your server;
- Use the following bash script:

```
zcat geoipify_ofac_cidr_2023_01_23.txt.gz > geoipify_ofac_cidr_2023_01_23_u
while IFS= read -r line; do echo "deny ${line};"; done <  geoipify_ofac_cid
rm -f geoipify_ofac_cidr_2023_01_23_uncompressed.txt
```

2. How to use data feeds with the Nginx geo module

Prerequisites:

- Nginx needs to be built with the **geo** module. You can check whether the Nginx was built with the **geo** module by running nginx -V and looking for the with-http_geoip_module flag. Also, you can check whether it's enabled via *'/nginx/modules-enabled*';
- Note that it works only with **if** clauses usage.

How to check:

```
Command: nginx -V 2>&1 | tr ' ' '\n' | egrep -i 'geo'
Output: --with-http_geoip_module=dynamic
```

Or:

```
Command: nginx -V 2>&1 | tr ' ' '\n' | egrep -i 'modules-path'
Output: --modules-path=/usr/lib/nginx/modules
Command: ls -lh /usr/lib/nginx/modules | grep geo
Output: -rw-r--r-- 1 root root  24K Nov 10 06:38
ngx_http_geoip_module.so
Command: cat /etc/nginx/modules-enabled/50-mod-http-geoip.conf
Output: load_module modules/ngx_http_geoip_module.so;
```

Example of *./mySite.conf* if the deny list resides in the default config folder:

```
location / {
    if ( $allowed_trafic = 'false') {
        return 403;
    }
}
```

Example if the deny list resides in the *./nginx.conf*:

```
include /etc/nginx/conf.d/*.conf;
```

Example of *my_deny_nginx_geo.conf*:

```
geo $remote_addr $allowed_trafic {
    default true;
    1.4.32.0/19 false;
}
```

How to convert the data feed to a deny list for the Nginx geo module?

To create *my_deny_nginx_geo.conf*:

- Download the data feed in CIDR notation to your server;
- Use the following bash script:

```
zcat geoipify_ofac_cidr_2023_01_23.txt.gz > geoipify_ofac_cidr_2023_01_23_u
while IFS= read -r line; do echo "${line} false;"; done < geoipify_ofac_cid
echo "geo \$remote_addr \$allowed_trafic {" > my_deny_nginx_geo.conf
echo "default true;" >> my_deny_nginx_geo.conf
cat my_deny_nginx_geo.conf.tmp >> my_deny_nginx_geo.conf
```

```
echo -n "}" >> my_deny_nginx_geo.conf
rm -f my_deny_nginx_geo.conf.tmp
rm -f geoipify_ofac_cidr_2023_01_23_uncompressed.txt
```

How to use data feeds with an Apache web server?

Enable the **rewrite** module with the *a2enmod* rewrite command. Example of *./mySite.conf* if the deny list does not reside in the default config folder:

```
<VirtualHost *:80>
    ServerName mysite.localhost.local
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    Alias /blocked "/var/www/blocked"
    <Directory "/var/www/blocked">
        AllowOverride All
        Require all granted
    </Directory>
    <IfModule mod_dir.c>
        DirectoryIndex index.php
    </IfModule>
    <Location /blocked>
        <RequireAll>
            Require all granted
            Include /etc/apache2/my_deny_apache2.conf
        </RequireAll> ErrorDocument 403 "<h3>Your IP is blocked.</h3>"
    </Location>
</VirtualHost>
```

Example of *my_deny_apache2.conf*:

```
Require not ip 1.0.1.0/24
Require not ip 1.0.2.0/23
Require not ip 1.0.4.0/32
Require not ip 1.0.8.0/21
Require not ip 1.0.16.0/32
Require not ip 1.0.32.0/19
Require not ip 1.0.64.0/32
```

How to convert the data feed to a deny list for Apache?

To create *my_deny_apache2.conf*:

- Download the data feed in CIDR notation to your server;
- Use the following bash script:

```
zcat geoipify_ofac_cidr_2023_01_23.txt.gz > geoipify_ofac_cidr_2023_01_23_u
while IFS= read -r line; do echo "Require not ip ${line}"; done < geoipify_
rm -f geoipify_ofac_cidr_2023_01_23_uncompressed.txt
```