

```

# BEGIN iThemes Security
#Quick ban IP. Will be updated on next formal rules save.
SetEnvIF REMOTE_ADDR "^203\.119\.101\.249$" DenyAccess
SetEnvIF X-FORWARDED-FOR "^203\.119\.101\.249$" DenyAccess
SetEnvIF X-CLUSTER-CLIENT-IP "^203\.119\.101\.249$" DenyAccess
order allow,deny
deny from env=DenyAccess
deny from 203.119.101.249
allow from all

# BEGIN Tweaks
# Rules to disable directory browsing
Options -Indexes

<IfModule mod_rewrite.c>
    RewriteEngine On

    # Rules to help reduce spam
    RewriteCond %{REQUEST_METHOD} POST
    RewriteCond %{REQUEST_URI} ^(\. *)wp-comments-post\.php*
    RewriteCond %{HTTP_REFERER} !^\. *
    RewriteCond %{HTTP_REFERER} !^http://jetpack\.wordpress\.com/jetpack-comment/ [OR]
    RewriteCond %{HTTP_USER_AGENT} ^$
    RewriteRule ^(\. *)$ - [F]
</IfModule>

# END Tweaks
# END iThemes Security
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
<files wp-login.php>
Order deny,allow
Deny from all

# Whitelist APNIC Secretariat IPs for login
Allow from 2001:0DD8:0012::/48
011...

```

```
Allow from 2001:0000:0000::/40
Allow from 2001:0DD8:000c::/48
Allow from 2001:0DD8:0009::/48
Allow from 2001:0DC0::/32
Allow from 203.119.101.0/24
Allow from 203.119.77.0/24
Allow from 203.119.95.0/24
Allow from 203.119.92.0/23
Allow from 203.119.86.0/24
Allow from 203.119.76.0/24
Allow from 203.119.42.0/24
Allow from 203.119.0.0/24
Allow from 202.12.29.0/24
</files>
<IfModule mod_headers.c>
# Caching JS/CSS/etc files for 3 hours
<FilesMatch "\.(css|js|png|jpg|jpeg)$">
Header set Cache-Control "max-age=10800, public"
</FilesMatch>
</IfModule>

# Being Redirects
Redirect 302 /2014/08/03/why-i-like-the-routing-manifesto/ /2014/08/10/why-i-like-the-
routing-manifesto/
Redirect 302 /lacnic-monc /2014/10/31/lacnic-community-discusses-iana-stewardship-
transition/
```