

rpm -Uvh

http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-11.noarch.rpm

yum install mod_security mod_security_crs

Edit ModSecurity configuration file `/etc/httpd/conf.d/mod_security.conf` and look for the `SecRuleEngine` Directive on the File and configured with the Desired Value.

On – Rules are activated

Off – Rules are Deactivated

DetectionOnly – Only Intercepts and logs Transactions

Since we want to Intercept and Block Attacks we configure it with On.

`SecRuleEngine on`

service httpd restart

To confirm that our web application firewall is working we should see something like this in our Apache error logs.

tail /var/log/httpd/error_log

You should see something like this:

```
[Sat Mar15 16 09:20:58 2014] [notice] ModSecurity for Apache/2.7.3  
(http://www.modsecurity.org/) configured.
```

```
[Sat Mar15 16 09:20:58 2014] [notice] ModSecurity: APR compiled version="1.3.9"; loaded  
version="1.3.9"
```

```
[Sat Mar15 16 09:20:58 2014] [notice] ModSecurity: PCRE compiled version="7.8 "; loaded  
version="7.8 2008-09-05"
```

```
[Sat Mar15 16 09:20:58 2014] [notice] ModSecurity: LUA compiled version="Lua 5.1"
```

```
[Sat Mar15 16 09:20:58 2014] [notice] ModSecurity: LIBXML compiled version="2.7.6"
```