IntruderIPAttempts

Learn how to use the IntruderIPAttempts config.txt directive to configure a security option in EZproxy. IntruderIPAttempts offers EZproxy administrators a simple and powerful security configuration option to limit unauthorized users from accessing resources through repeated attempts to generate valid credentials. At the same time, it allows room for the possibility that a legitimate user has forgotten their credentials and should not be locked out of the system completely. This directive does not safeguard against stolen or misused valid credentials.

When used as an event in combination with the Audit directive, the IntruderIPAttempts directive can help EZproxy administrators to identify compromises to EZproxy security and put stronger security protocols in place to prevent the security threat.

IntruderIPAttempts is a position-dependent config.txt directive that typically appears toward the top. The directive is used to enable intruder detection based on source the IP address to enhance EZproxy security. You can customize the parameters that will cause a user to be blocked from EZproxy based on invalid credentials and IP address using the directive qualifiers.

Note: This directive replaced the IntruderAttempts and IntruderTimeout directives.

Qualifiers

The following qualifiers should be added to your IntruderIPAttempts directive to specify when to block a user who repeatedly attempts to use invalid credentials from the same IP address. The italicized word should be replaced with the numerical value you would like to use as a parameter.

<table>
<thead>
<tr>
<th>QUALIFIER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>-interval=minutes</td>
<td>Number of minutes in which the count from an IP address must be reached in order for EZproxy to start blocking all login attempts from that address.</td>
</tr>
<tr>
<td>-expires=minutes</td>
<td>Number of minutes which must pass with no further login attempts from a blocked IP address before EZproxy will stop blocking login attempts from that address.</td>
</tr>
<tr>
<td>count</td>
<td>Number of login attempts from an IP address using invalid information that must occur during the -interval before EZproxy starts blocking all login attempts from that address.</td>
</tr>
</tbody>
</table>
Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-reject=rejectcount</td>
<td>Number of login attempts from an IP address using invalid information that must be reached during the -interval before EZproxy treats the IP address as a RejectIP address, blocking all further logins from that address until the restriction is manually cleared using the option on the EZproxy Administration Page.</td>
</tr>
</tbody>
</table>

Syntax

```
IntruderIPAttempts -interval=5 -expires=15 20
```

Examples

If you are uncertain about initial security configurations to use with the IntruderIPAttempts directive, you can begin with the following:

```
IntruderIPAttempts -interval=5 -expires=15 20
```

This will provide you with a baseline security setting that will block any user who tries to log in from a single IP address with invalid information more than 20 times within a 5 minute period of time. After 15 minutes, if no other users attempt to log in from that IP address, EZproxy will no longer block users from that IP address. These are good baseline parameters to use because users legitimately forget passwords, and these timeframes and limits allow them a sufficient amount of time to test several passwords, and if they fail to enter the correct credentials in this time period, they have to wait only 15 minutes to try again.

After this directive has been added to your config.txt file, you should also add Audit Most to your config.txt file so you can monitor your audit logs from your admin page by clicking on the View audit events link. You will see a table similar to the following:

```
DATE/TIME | EVENT          | IP          | LOCATION     | USERNAME      | OTHER                           |
----------|----------------|-------------|--------------|---------------|---------------------------------|
11:00:17  | System         |             |              |               | Startup                         |
11:00:17  | System         |             |              |               | Purged audit file 20140930.txt  |
11:00:56  | Login.Success  | 127.0.0.1   | US OH Dublin | ypAvVbCo28nsw7y |                                |
11:04:00  | Login.Intruder.IP | 123.456.789.101 | US OH Dublin | ghAvILFw30lwk09 |                                |
11:10:45  | Login.Success  | 123.789.101.112 | US OH Dublin | ifJlwElwo50jkl19 |                                |
```
Look for any events labeled Login.Intruder.IP. If you see repeated blocked logins from the same IP address, you may first want to determine if this IP address and user is a valid user who is having difficulty understanding and logging in to your EZproxy resources. If you determine that this is not a legitimate user, you may want to consider adding a -reject= qualifier to your directive statement so that a user who repeatedly tries to log in from a specific IP address with invalid credentials will be blocked as if that IP address were configured as a RejectIP. Your directive statement for this configuration should be as follows:

```
IntruderIPAttempts -interval=5 -expires=15 -reject=100 20
```

This will maintain the same parameters from blocking as above, but will place a continuous block on the offending IP address that must be cleared manually from the /admin EZproxy administration page. If you find that one particular IP address continues to cause problems, you might want to add a RejectIP for that address to block it permanently.

**Related directives**

- Audit
- IntruderUserAttempts
- RejectIP