Linux DDoS Protection / Brute Force Throttling

For older operating systems (ie. Ubuntu 16), you'll want to replicate similar behavior via IPTables. Newer operating systems have made the mode to UFW, so we'll only cover UFW in this document. If you're interested in implementing IPTables on an older operating system, you may submit a request for instruction to support@arcanestrategies.com.

This document assumes that you've already set up UFW rules for allowing or denying port accessibility as this will only cover traffic throttling.

1. First open your UFW rules for editing: **$ sudo vi /etc/ufw/before.rules**

2. Now set your HTTP and HTTPS connection limits. You'll find a few sections which begin with "-A ufw-http". You'll want to edit them as follows:

    a. Increase your Connections per Class C network. The "--connlimit-above" value determines how many simultaneous connections may exist on a class c network, which could be any number of different users. The default is 50, so if you plan on supporting a larger load (a few hundred or a few thousand), you'll need to increase this accordingly.

    b. Keep a low number of connections per IP. You'll see a couple lines ending in "--conn_per_ip" (--set and --update). The second one should indicate the number of hits (--hitcount) permitted per number of seconds (--seconds). The math here is pretty basic, 20 hits over 5 seconds would mean 4 hits per second from the same IP, which is fairly reasonable but will limit your users if you have multiple users on the same network (ie. your office), so that might be a bit low but not too far off for your average website. You'll want this to accommodate your expected traffic needs (per above). Experiment with this using your best judgment.

    c. Keep a low number of packets per IP. After connections per IP, you'll want to set the packets per IP. The logic here is the same. Each connection has multipe packets, so if you're looking at 20 connections per 5 seconds, you might be looking at five-to-ten times that for packets (ie. 20-40 packets per 1 second).

...Next Page...

Linux DDoS Protection / Brute Force Throttling

1. If you've used IPtables for your rate throttling, you may notice the UDP flood and SSH are not covered here. UDP flood does not exist within the most recent version of UFW. SSH protection should be covered through fail2ban. Here are some of our fail2ban suggestions:

    a. Open fail2ban for editing. Each service/protocol is identified within brackets and followed by their corresponding variables: **$ sudo vi /etc/fail2ban/jail.local**

    b. **[default]**
    "maxretry = " This is the default number for all of your services which are subject to attack (ftp, ssh, mysql, ldap, etc). We suggest setting this to a number which is reasonably high but low enough to block a brute force attack. A brute force attacker might perform thousands of attempts whereas a regular user might fail to login 3 or 4 times before considering a different route or password change, so a figure in the double-digit range seems reasonable.

    c. **[sshd]** - If you're using vsftp, pure-ftp, or any other ftp access aside from ssh, you'll want to find those corresponding sections and repeat this process as needed (your ftp ports will be different than ssh; by default ftp is port 21)
    "port = " If you are using a different port for SSH update this to the port you're using

    d. **[postfix]**
    "maxretry = " If using postfix, we suggest setting max retries set to 10. This will protect you from flooding the mail server from bounces, incorrect configuration, or if your server gets compromised as a pass-through spammer.

NOTE: If you're using nagios, which we recommend for monitoring, you'll configure that here as well. If you are installing fail2ban from scratch, you'll find a lot of errors when checking the status as fail2ban will require logs for all services it monitors, even if you comment them out in the configuration. To overcome these, you can choose to create these logs and/or create a master junk log and set each of these configurations to that master junk log. Be sure to "restart" fail2ban after changes and then check "status" to verify if the configuration changes fixed the problem. It must pass to properly run.

support@arcanestrategies.com
(541) 649-2508

Arcane Strategies
7 E. Congress St. #804
Savannah, GA 31401