Nathan Christensen-Padilla

Adrianna Holden-Gouveia

Linux Administration

12/12/2021

Firewalls DDOS Protection

There are few a different ways I could prevent a ddos attack using iptables like blocking all invalid packets that come into my server and another tactic I could use is a rule that blocks packets that are not a SYN packets or ESTABLISHED tcp connections. Also, blocking packets that have unusual flags that normal internet traffic wouldn’t use. Another very important iptable rule is blocking brute force attempts like limiting the amount of attempts someone can do in a short period of time, ie spamming my server with SSH.

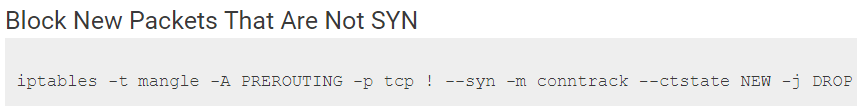
I think the best way to prevent or atleast reduce the load of DDOS attacks is to do what I said above but also have backup scripts that you can run for different kinds of attacks. The reason you would want backup scripts and not have certain rules up all the time is because it could block legitimate traffic which would be bad for the server. Overall, making sure that I monitor my server and look for signs of DDOS attacks is very important, because catching the problem early can really help me delpoy my counter-measures before anything too bad happens.

Sources:

[How To Build Your Own DDoS Protection With Linux & IPtables in 2021 (javapipe.com)](https://javapipe.com/blog/iptables-ddos-protection/)

This website provides really good examples of iptable commands that I could use like:

Text

Description automatically generated with low confidenceGraphical user interface, text

Description automatically generated

[How to Prevent DDoS Attacks: 7 Tried-and-Tested Methods (phoenixnap.com)](https://phoenixnap.com/blog/prevent-ddos-attacks)

This website provided a lot of information about DDOS attack and some ways of preventing them it was really informative.