Installing and Configuring Linux DDOS Deflate

DDOS (Distributed Denial of Service) is a type of DOS (Denial of Service) attack in which an online service is made unavailable to its intended users. This is a frequently encountered attack due to availability of various tools online that are made to target a wide variety of important resources. These tools are easy to use and are freely available on the internet in a simple google search. These tools make UDP, TCP or HTTP requests to the victim server.

Types of DDOS attacks:

1) Application Layer DDOS attack

2) Protocol DDOS attack

3) Volume based DDOS attack

Application Layer DDOS attack: Application Layer DDOS attack is a type of DDOS attack which targets the application layer of OSI model. The size of these attacks are measured in requests per second (RPS).

Protocol DDOS attack: Protocol DDOS attack targets server resources rather than bandwidth.

Volume based DDOS attack: Volume based DDOS attack uses a variety of different techniques to saturate bandwidth of the attacked site, so other visitors can access it. It eventually leads the server to crash.

There are three ways to defend against DDOS:

1) Attack Prevention and Preemption: It is done before the attack.

2) Attack Detection and Filtering: It is done during the attack.

3) Attack Source: It can be done during and after the attack.

DDOS Deflate

DDOS Deflate is a lightweight bash shell script designed to block DOS attacks. It does not fully protect against large DDOS attacks, but it is helpful. It uses netstat command to track and monitor all the IP addresses making connections to the server. Whenever it detects the number of connections from a single node exceeding certain pretest limits which are defined in the configuration file, the script will automatically block that IP address through IP tables or APF according to the configuration. We can use the command below to list IP address connected to the server along with their total number of connections.

```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

DDOS Deflate Installation

```
cd /usr/local/src/
wget http://www.inetbase.com/scripts/ddos/install.sh
chmod 0700 install.sh
./install.sh
```

Edit configuration file

```
vi /usr/local/ddos/ddos.conf
```

Start DDOS Deflate

```
/usr/local/ddos/ddos.sh -c
```

Unistall DDOS Deflate

```
wget http://www.inetbase.com/scripts/ddos/uninstall.ddos
chmod 0700 uninstall.ddos
./uninstall.ddos
```

Features of DDOS Deflate

1) Whitelist IP addresses, via /usr/local/ddos/ignore.ip.list.

2) Simple configuration file /usr/local/ddos/ddos.conf

3) IP addresses are automatically unblocked after a preconfigured time limit.

4) Script can run at a chosen frequency via the configuration file.

5) Receive email alerts when IP addresses are blocked.

6) Support APF, CSF and iptables.

7) Helps to reduce the amount of processes opened by attackers using tcpkill.

Options of ddos deflate

To show the help screen

```
# ddos –help
```

Create cron job to run the script regularly

```
# ddos –cron
```

Display whitelisted IP addresses

```
#ddos -l | –ignore-list
```

Display currently banned IP addresses.

```
# ddos -b | –bans-list
```

To initialize a daemon to monitor connections.

```
# ddos -d | –start:
```

To Stop the daemon.

```
# ddos -s | –stop
```

To show status of daemon and pid currently running.

```
# ddos -t | –status
```

To display active connections to the server.

```
# ddos -v | –view
```

To block all IP addresses making more than N connections.

```
# ddos -k | –kill:
```

If you need any further assistance please contact our support department.

LEAVE A COMMENT

Comment...

Name (required)

Email (required)

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

DDOS

- DDOS Prevention Settings in CSF firewall
- What is MAC Flooding? How to prevent it?
- What is IP Spoofing? Types of IP Spoofing
- What is SYN Flood attack and how to prevent it?

- How to Troubleshoot a DDoS Attack?

HOSTING SERVICES

Standard Web Hosting
Pro Hosting (reseller)
ASP.Net Hosting
Email Hosting
cPanel Hosting
Non Profit Hosting
Student Web Hosting
Website Builder
E-Commerce

VPS & CLOUD

VPS Home
Windows VPS
Backups
Bread Basket (webuzo)
cPanel VPS
Debian VPS
CentOS VPS

DEDICATED SERVERS

Dedicated Home

Storage Servers
10Gbps Dedicated Servers
GPU Dedicated Servers
Rapid Deploy Servers

WHY US

About Us
Network
Datacenter
Our Team
Reviews

POPULAR APPS

Wordpress Hosting
Joomla Hosting
Magento Hosting
Prestashop Hosting

CLIENT SERVICES

Contact Us
Control Panel
Affiliate Program

TIPS ARTICLES

Getting Started
WordPress Tutorials
Migrating to InterServer
Email Tutorials
Joomla Tutorials
E-Commerce Tutorials

LATEST BLOG POST

New Plesk Toolkits and Features
Two Factor Authentication: A Security Must-Have
VPS Control Panel Management Made Easy

Payments We Accept