HOW TO PREVENT DDOS ATTACK ON CENTOs 7

CentOS DDoS protection – A guide to secure your server from DDoS!

DDoS(Distributed Denial Of Service) is an advanced version of DoS(Denial Of Service).

FAIL TO BAN

- `sudo yum install epel-release -y – (Installing Extra Packages for Enterprise Linux)`
- `sudo yum install fail2ban -y (Installing Fail2BAn)`
- `sudo systemctl enable fail2ban (use systemctl to enable the fail2ban service)`
- `sudo nano /etc/fail2ban/jail.local (create jail.local file)`
- `paste the following`

```
[DEFAULT]
# Ban hosts for one hour:
bantime = 3600

# Override /etc/fail2ban/jail.d/00-firewalld.conf:
banaction = iptables-multiport

[sshd]
enabled = true

[apache]
enabled  = true
port     = http,https
filter   = apache-auth
#logpath  = /var/log/apache*/*error.log (specify
your application log path)
maxretry = 6
findtime = 600

[php-url-fopen]
enabled = true
port    = http,https
filter  = php-url-fopen
#logpath = /var/log/apache*/*access.log (specify
your application log path)

[apache-overflows]
enabled  = true
```

```
port     = http,https
filter   = apache-overflows
#logpath  = /var/log/apache*/*error.log (specify
your application log path)
maxretry = 2

[apache-badbots]
enabled  = true
port     = http,https
filter   = apache-badbots
#logpath  = /var/log/apache*/*error.log (specify
your application log path)
maxretry = 2

[apache-nohome]
enabled  = true
port     = http,https
filter   = apache-nohome
#logpath  = /var/log/apache*/*error.log (specify
your application log path)
maxretry = 2

ignoreip = 127.0.0.1/8 10.10.11.155 (IP that
fail2ban shuld ignore)

[postfix-rbl]
filter   = postfix[mode=rbl]
port     = smtp,465,submission
logpath  = %(postfix_log)s (specify your application
log path)
backend  = %(postfix_backend)s
maxretry = 1
```

- systemctl restart fail2ban (restart fail2ban)
- fail2ban-client status (check fail2ban status)
- fail2ban-client status sshd (check fail2ban per application)

1. result of fail2ban-client status sshd

```
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     139
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 1
   |- Total banned:     31
   `- Banned IP list:   10.10.10.11
[root@localhost ~]#
```

2. result of fail2ban-client status apache

```
[root@localhost ~]# sudo fail2ban-client status apache
Status for the jail: apache
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@localhost ~]#
```

3. iptables -S (all rules for fail2ban accept/reject connections)

```
[root@localhost ~]# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-N FORWARD_IN_ZONES
-N FORWARD_IN_ZONES_SOURCE
-N FORWARD_OUT_ZONES
-N FORWARD_OUT_ZONES_SOURCE
-N FORWARD_direct
-N FWDI_public
-N FWDI_public_allow
-N FWDI_public_deny
-N FWDI_public_log
-N FWDO_public
-N FWDO_public_allow
-N FWDO_public_deny
-N FWDO_public_log
-N INPUT_ZONES
-N INPUT_ZONES_SOURCE
-N INPUT_direct
-N IN_public
-N IN_public_allow
-N IN_public_deny
-N IN_public_log
-N OUTPUT_direct
-N f2b-sshd
-A INPUT -p tcp -m multiport --dports 22 -j f2b-sshd
-A INPUT -p tcp -m multiport --dports 22 -j f2b-sshd
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -j INPUT_direct
-A INPUT -j INPUT_ZONES_SOURCE
-A INPUT -j INPUT_ZONES
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i lo -j ACCEPT
-A FORWARD -j FORWARD_direct
-A FORWARD -j FORWARD_IN_ZONES_SOURCE
-A FORWARD -j FORWARD_IN_ZONES
-A FORWARD -j FORWARD_OUT_ZONES_SOURCE
-A FORWARD -j FORWARD_OUT_ZONES
```