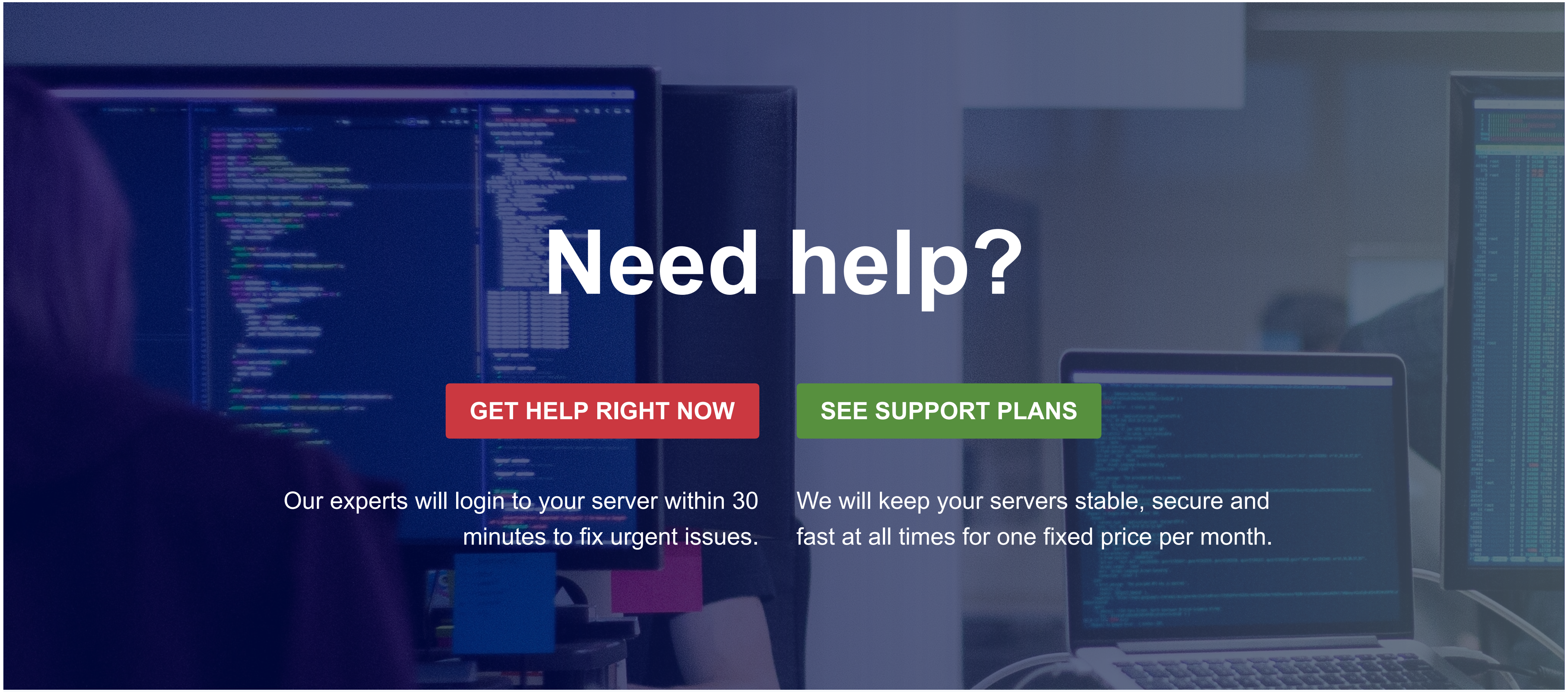

Need help?

GET HELP RIGHT NOW

SEE SUPPORT PLANS

Our experts will login to your server within 30 minutes to fix urgent issues.

We will keep your servers stable, secure and fast at all times for one fixed price per month.

Leave A Message

Prevent DDoS in Apache – Steps to safeguard your web server from DDoS

by Lakshmi Vijayakumar | 07 January , 2019

It’s a fact that the threat of DDoS attacks is increasing!

Since Apache is a widely used web server, it can fall as the prime victim of DDoS.

Quite a terrible situation, right? So, what’s the smart decision here?

Even though, there is no perfect solution to prevent Apache DDoS attacks, we can defend it to a great extent.

At Bobcares, we help our server owners to harden and secure their web servers as part of our Dedicated Support Services for web hosts.

Today, we’ll discuss the top 8 methods to *prevent Apache DDoS* attacks.

What is DDoS? – A Brief Explanation

Before we go ahead, let’s see what DDoS is.

DDoS(Distributed Denial Of Service) tries to deny important services running on the system by sending heavy traffic, so that the server can’t handle it.

What is DDoS attack?

Similarly, in a web server DDoS attack, attacker exploits HTTP *GET* or *POST* requests to attack the web server or application.

Consequently, it leads to service down time, reputation damage, financial loss, and more.

So, it’s really important to protect the web server from DDoS attacks.

How to prevent DDoS attacks in Apache?

Let’s now discuss how our Dedicated Support Team enable DDoS protection on Apache web servers.

1) Install mod_evasive Apache module

The ***mod_evasive*** Apache module offers a stronger way of protecting the web server against DDoS, DoS, and brute force attacks.

It tracks the IPs and pages requested to the Apache web server. And, blocks the traffic from that IP when the threshold is reached on the page or site.

As a result, the website displays 403 Forbidden errors.

Below are some of the mod_evasive parameters that our Security Experts tweak in ***mod_evasive.conf*** file to prevent DDoS attacks.

```
DOSHashTableSize
DOSPageCount
DOSSiteCount
```

```
DOSPageInterval
DOSSiteInterval
DOSBlockingPeriod
```

2) Install Mod_security module

Mod_security is an open source ***WAF(Web Application Firewall)*** that easily works with Apache.

It uses various protection rules to monitor the HTTP traffic and block suspicious/unwanted traffic, SQL injection, etc.

At Bobcares, we help server owners to integrate mod_security with Apache.

In addition to that, we set custom protection rules and add them to the mod_security configuration file ***/usr/local/apache/conf/mod_security.conf***.

For example, our Support Engineers tweak the following mod_security parameters to limit the maximum data that can be posted on a web application, .

```
SecRequestBodyLimit
SecRequestBodyNoFilesLimit
```

3) Install DDoS Deflate

DDoS Deflate tool is an effective way of mitigating DDoS attacks for a limited number of websites.

It's a bash script that uses ***netstat*** to identify and ban IPs that open too many connections to the

This application runs the following command to check the number of connections.

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

And, if the number of connections exceeds the threshold limit, it will automatically block that IP on the server.

Additionally, our Support Engineers tweak the DDoS Deflate configuration file "***/usr/local/ddos/ddos.conf***" to adjust the parameters like threshold connection limit, frequency at which the script runs, etc.

4) Software firewall

Similarly, DDoS attacks in Apache can be prevented by tweaking some parameters in the server firewall.

For example, in CSF, we enable and tweak parameters such as ***SYNFLOOD*** and ***PORTFLOOD*** to limit the connections on Apache web server port.

Moreover, we tweak CSF connection tracking parameters like ***CT_LIMIT, CT_INTERVAL, CT_BLOCK_TIME***, etc. to limit the number of connections.

In the same way, we configure APF and iptables to mitigate DDoS.

For example, in iptables, we set rules to rate limit the number of connections on Apache port 80.

```
iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 20 -j
REJECT --reject-with tcp-reset
```

And, if the number of connection exceeds the threshold, the IP is blocked on the server.

5) Install Fail2ban

Fail2ban is a good option to prevent DDoS attacks in Apache.

It uses a list of regular expressions and checks against server logs. And, if connections exceed the threshold values, it blocks such IP addresses in the firewall.

Also, Fail2ban uses jails to determine which services must be protected. So, our Security Engineers help server owners set up custom jails to enable Apache DDoS protection.

For example, we add the following code in fail2ban configuration file ***/etc/fail2ban/jail.local*** to enable Apache DDoS jail.

```
[apache]
enabled = true
port = http,https
filter = apache-auth
logpath = /var/log/apache2/*error.log
maxretry = 4
findtime = 500
ignoreip = 10x.12x.1xx.xx7
```

6) Tweak Apache Configuration

In addition to that, our Support Experts also tweak certain Apache configuration parameters to mitigate DDoS problems.

We tune the Apache parameters like *RequestReadTimeout, Timeout, KeepAliveTimeout*, etc. to reduce the impact of DDoS attacks.

For example, we lower *the KeepAliveTimeout* parameter on sites that are subject to DDoS attacks. Similarly, we tune *MaxRequestWorkers* directive to allow the server to handle maximum number of simultaneous connections without running out of resources.

However, we can't blindly tweak these parameters, so we analyze the server resources and traffic before tweaking these parameters.

7) Sysctl based protection

Another important step is to tweak the values set for *SYN_SENT, SYN_RECV, TIME_WAIT and FIN_WAIT* by modifying the below parameters in the ***/etc/sysctl.conf*** file.

```
net.ipv4.tcp_syncookies
net.ipv4.tcp_fin_timeout
net.ipv4.tcp_window_scaling
net.ipv4.tcp_sack
```

8) Setup Load balancer

Another best way to prevent Apache DDoS problems is by using load balancers such as HAPro

At Bobcares, our Server Administration Team help server owners setup load balancers on their servers.

In addition to that, we limit the number of connections per user, limit the HTTP request rate, etc. to mitigate DDoS attacks on web servers.

Conclusion

It's hard to recover from DDoS attacks. That's why protecting your web server against DDoS attacks is important. Today, we've discussed the 8 different steps that our Dedicated Support Engineers used to prevent DDoS in Apache.

Categories: Technical Support

Tags: DDoS DDoS Attack DDoS Protection DDoS Security Denial Of Service Attack Security Server Abuse

Submit a Comment

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

1 + □ = seven ⟳

SUBMIT COMMENT

Leave A Message

Search our blog

Leave A Message

support.

Tech support can keep you busy all day long. That is time you could use to focus on your business. Leave your end-user support to us, and use that time to focus on the growth and success of your business.

TALK TO SALES

Or click here to learn more.

Related Posts

How to use Fail2ban for securing Apache web server from 404 attacks?

DDoS prevention in Nginx – How to secure your server from DDoS attacks?

Shell shock rescue – Tracing a bandwidth spike to outbound DDoS through the infamous Bash vulnerability

CentOS DDoS protection – A guide t your server from DDoS!

Leave A Message

Preventing DDoS Attacks

Email

SIGN UP FOR EMAILS

Proudly based in India and the USA.

☎ 1-800-383-5193

sales@bobcares.com

Leave A Message

INFORMATIONWE ARE AT

- Contact Us
- About Us
- Partners
- AUP
- Privacy Policy
- Terms of Service

- Poornam Inc.
  202 East Earll Drive, Suite 410,
  Phoenix, AZ 85012
- Poornam Info Vision Pvt Ltd,
  VC Valley Phase II, CSEZ PO,
  Cochin, Kerala, India -682037
  https://bobcares.in/

LATEST BLOG POSTS

- Top 3 ways for Google cloud compute engine ssh access
  Posted on: 2019-08-18
- Smart ways to set up OpenCart SMTP
  Posted on: 2019-08-17
- AutoSSL DCV failure – Quick ways to fix it
  Posted on: 2019-08-16
- How to quickly setup Whmcs email piping?
  Posted on: 2019-08-15

Leave A Message

- Zen Cart showing blank page – How we nailed it in a faster way

  Posted on: 2019-08-14

Email

SIGN UP FOR EMAILS

Leave A Message