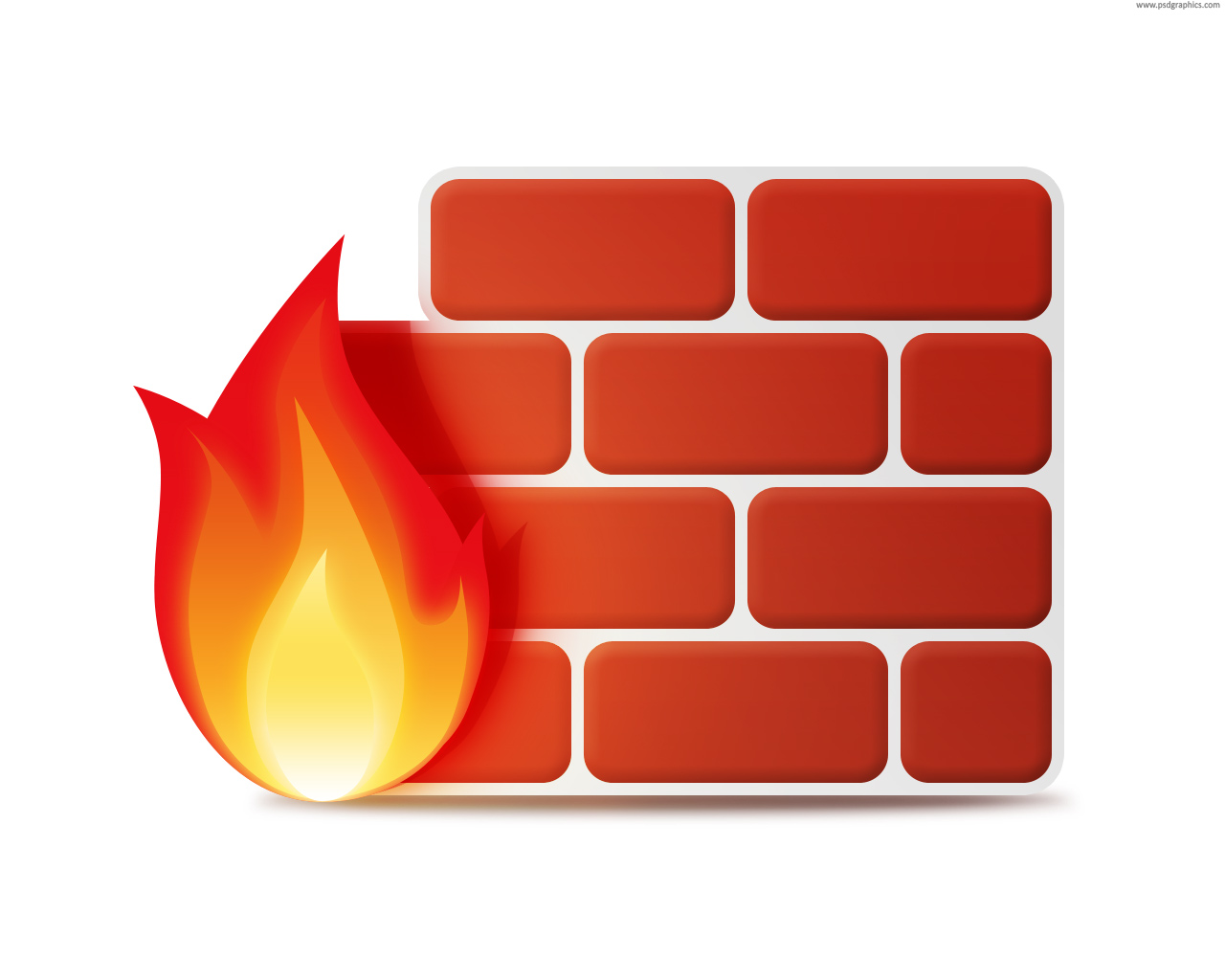
Created in the cloud with Aspose.Words for Cloud. http://www.aspose.com/cloud/word-api.aspx

# Firewall Protection

Published Date : September 8, 2016  
Author : tayo

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet



A firewall monitors all of the traffic entering your computer network. A two-way firewall does double duty and monitors the traffic exiting your network as well. Information is sent over networks in packets. Those packets are what the firewall investigates to determine if there’s something they contain that’s potentially hazardous to your network’s security. Even you as the sender could transmit something bad, without knowing it, which is why it’s important to have a firewall police the contents.

**Benefits of Firewall**

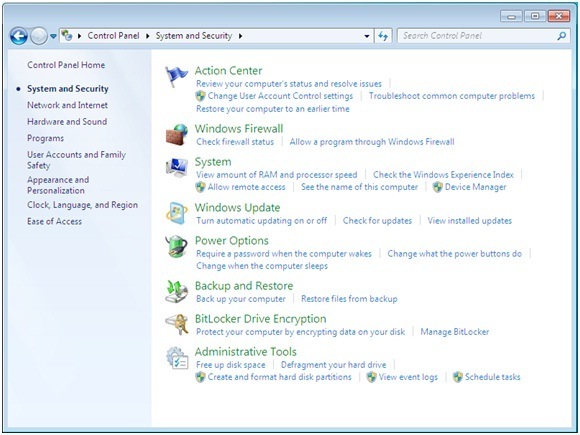
**1)**Blocks Trojans  
A firewall helps block Trojan horses. These types of intruders latch onto your computer files, and then when you send out a file, they go along for the ride to do more damage at the destination. Trojans are especially dangerous because they silently transmit what they uncover about you to a Web server. You’re oblivious to their presence until strange things start happening to your computer. A firewall blocks them from the outset, before they have a chance to infect your computer.

**2)**Stops Hackers  
Having a firewall keeps hackers out of your network. Without firewall security, a hacker could get a hold of your computer and make it a part of what’s called a botnet, which is a large group of computers used to conduct illicit activity, such as spreading viruses. While hackers represent an extreme group, individuals who you may not suspect, such as neighbors, can also take advantage of an open Internet connection you may have. A firewall prevents such peeping-tom intrusions.

**3)**Stops Keyloggers  
Having firewall security will reduce the risk of keyloggers monitoring you. A keylogger is spyware software that cybercriminals try to put on your computer so they can target your keystrokes. After they can identify what you’re typing in and where, they can use that information to do the same thing. This knowledge can help them log in to your private online accounts.

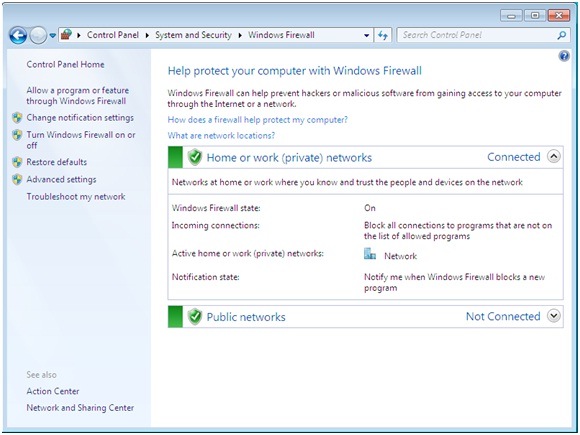
**How to enable Firewall on your windows computer**

1. From the Start menu, click **Control Panel**, then click **System and Security.**
2. Under Windows Firewall, select either **Check firewall status** to determine whether the firewall is turned on or off, or **Allow a program through Windows Firewall** to allow a blocked program through the firewall.



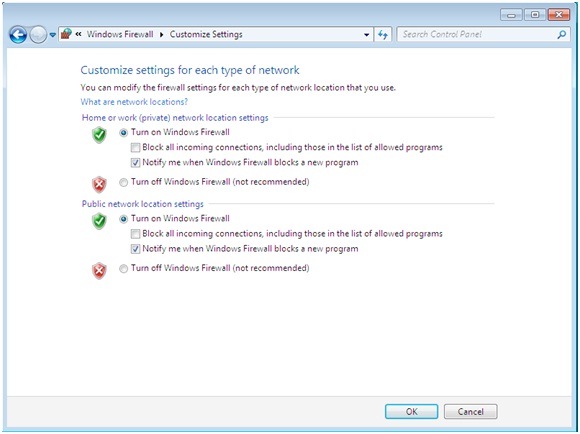
**2.** Select program features.

1. Click **Turn Windows Firewall on or off** from the left side menu.
2. Configure the settings for your home/work (private) or public network.
3. Click **OK** to save your changes.



**3.** Choose firewall settings for different network location types.

1. Turn on Windows Firewall for each network location you use – **Home or work (private)** or **Public.**
   * Click **What are network locations?** for more information on network types.
   * **Note:** Domain network locations are controlled by your network administrator and can’t be selected or changed.
2. Select **Turn on Windows Firewall** under the applicable network location type (in image below, both locations are selected).
3. Select **Notify me when Windows Firewall blocks a new program** for each network type, if the box is not already checked.
4. Click **OK** to save your changes.



### Comments

# Prevent Hackers from impersonating you by sending emails that looks like yours

Published Date : September 8, 2016  
Author : tayo



There are chances that you have received an email claiming to be from someone or an organization but you later found out that the email was a scam and not real. Cyber criminals have devised ways to send fake emails and make it seem real by exploiting a flaw in the way the email system works. The email work using an outdated protocol called the SMTP or Simple Mail Transfer Protocol.

Criminals can easily use free malicious software to send fake emails and make them appear real by the process we call email spoofing.

To prevent email spoofing and stop hackers from sending fake emails to your users thereby making it look real you can enable some of these three options from your web hosting control panel.

**Sender Policy Framework (SPF):**

The ‘Sender Policy Framework’ (SPF) is an email validation system, designed to prevent unwanted emails sent using a spoofing system.

Basically, SPF helps to weed out abusive emails and also detect email forgery. It allows  domain owners to publish trusted IP addresses that are authorized to send emails from the specified domains. For example, if my website “www.xyz.com” is hosted on the IP address 192.168.0.1 I can make sure only the ip address 192.168.0.1 is able to send emails out. Whenever a cyber criminal tries to send an email impersonating my website it would either end up in the spam box or gets rejected.

To configure SPF be sure to ask your web hosting company to help you set these up.

### Comments

# Secure Coding Practices

Published Date : September 8, 2016  
Author : tayo

We would be sharing with you 12 secure coding practices that cuts across different programming languages and have over time, been proven to mitigate security risks that are associated with coding. These practices, if properly implemented, would increase your protection against the numerous attacks that applications face daily.

### Top 12 Secure Coding Practices

1. **Validate input.** ALWAYS validate input. Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software [vulnerabilities](https://www.securecoding.cert.org/confluence/display/c/BB.+Definitions" \l "BB.Definitions-vulnerability). Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user controlled files.
2. **Heed compiler warnings.** Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code . Use static and dynamic analysis tools to detect and eliminate additional security flaws.
3. **Architect and design for security policies.** Create a software architecture and design your software to implement and enforce security policies. For example, if your system requires different privileges at different times, consider dividing the system into distinct intercommunicating subsystems, each with an appropriate privilege set.
4. **Keep it simple.** Keep the design as simple and small as possible  Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use. Additionally, the effort required to achieve an appropriate level of assurance increases dramatically as security mechanisms become more complex.
5. **Default deny.** Base access decisions on permission rather than exclusion. This means that, by default, access is denied and the protection scheme identifies conditions under which access is permitted .
6. **Manage Users, Sessions and Permissions.** Every process should execute with the the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time. This approach reduces the opportunities an attacker has to execute arbitrary code with elevated privileges.
7. **Sanitize data sent to other systems.** Sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components. Attackers may be able to invoke unused functionality in these components through the use of SQL, command, or other injection attacks. This is not necessarily an input validation problem because the complex subsystem being invoked does not understand the context in which the call is made. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.
8. **Practice** **defense in depth.** Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can prevent a [security flaw](https://www.securecoding.cert.org/confluence/display/c/BB.+Definitions" \l "BB.Definitions-securityflaw) from becoming an exploitable vulnerability and/or limit the consequences of a successful [exploit](https://www.securecoding.cert.org/confluence/display/c/BB.+Definitions" \l "BB.Definitions-exploit). For example, combining secure programming techniques with secure runtime environments should reduce the likelihood that vulnerabilities remaining in the code at deployment time can be exploited in the operational environment.
9. **Use effective quality assurance techniques.** Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should all be incorporated as part of an effective quality assurance program. Independent security reviews can lead to more secure systems. External reviewers bring an independent perspective; for example, in identifying and correcting invalid assumptions .
10. **Adopt a secure coding standard.** Develop and/or apply a secure coding standard for your target development language and platform.
11. **Define security requirements.** Identify and document security requirements early in the development life cycle and make sure that subsequent development artifacts are evaluated for compliance with those requirements. When security requirements are not defined, the security of the resulting system cannot be effectively evaluated.
12. **Model threats.** Use threat modeling to anticipate the threats to which the software will be subjected. Threat modeling involves identifying key assets, decomposing the application, identifying and categorizing the threats to each asset or component, rating the threats based on a risk ranking, and then developing threat [mitigation](https://www.securecoding.cert.org/confluence/display/c/BB.+Definitions" \l "BB.Definitions-mitigation) strategies that are implemented in designs, code, and test cases

This guide was written to serve as a secure coding kick-start tool and easy reference, to help development teams and individual developers quickly understand secure coding practices.

### Comments

# Protecting your website against attacks using web application firewall

Published Date : September 8, 2016  
Author : tayo

### 

### Introduction

#### In this tutorial, we will show you how to use CloudFlare’s free tier service to protect your web servers against ongoing HTTP-based DDoS attacks by enabling “I’m Under Attack Mode”. This security mode can mitigate DDoS attacks by  verifying the legitimacy of a connection before passing it to your web server.

## Prerequisites

This tutorial assumes that you have the following:

* A web server
* A registered domain that points to your web server
* Access to the control panel of the domain registrar that issued the domain

You must also sign up for a CloudFlare account before continuing. Note that this tutorial will require the use of CloudFlare’s nameservers.

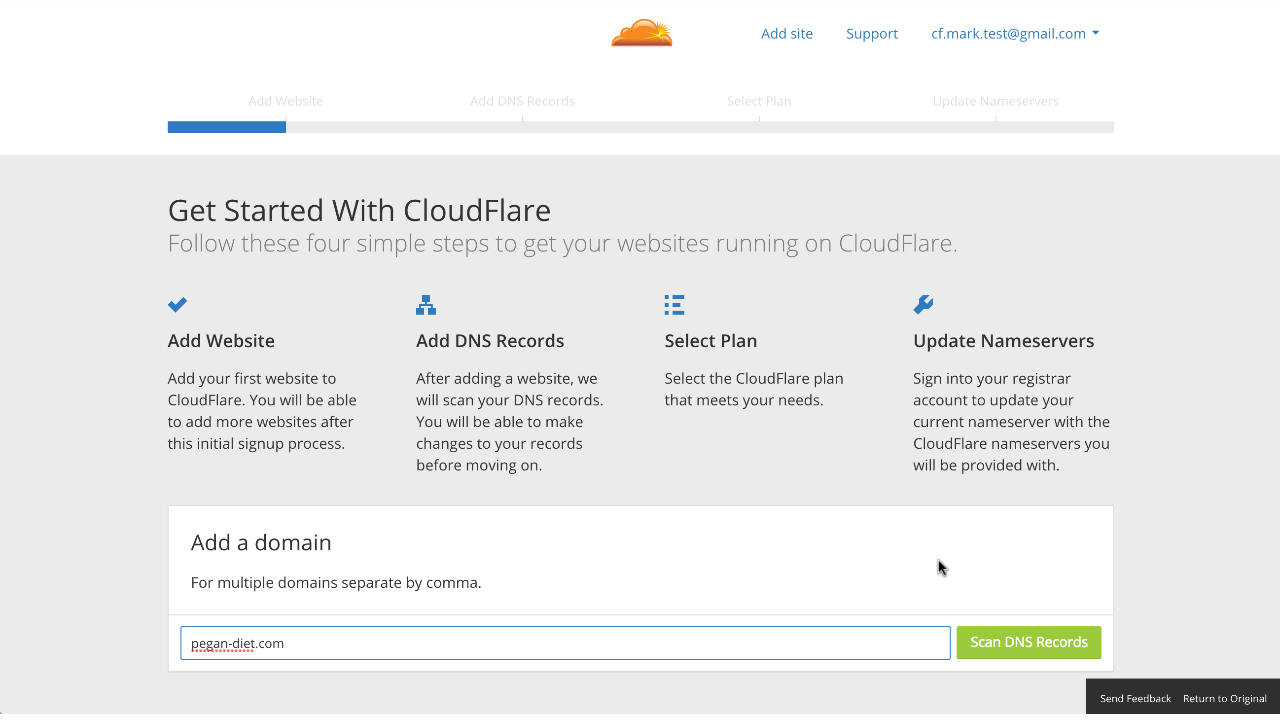
## Configure Your Domain to Use CloudFlare

Before using any of CloudFlare’s features, you must configure your domain to use CloudFlare’s DNS.

If you haven’t already done so, log in to CloudFlare.

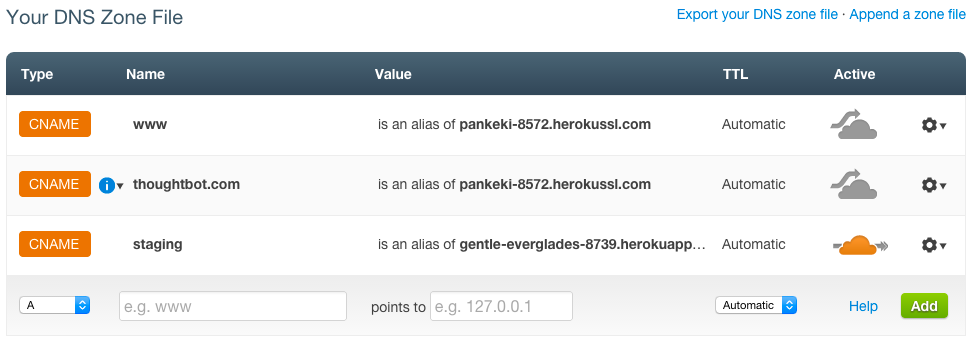
### Add a Website and Scan DNS Records

After logging in, you will be taken to the Get Started with CloudFlare page. Here, you must add your website to CloudFlare and Begin Scan:



The next page shows the results of the DNS record scan. Be sure that all of your existing DNS records are present, as these are the records that CloudFlare will use to resolve requests to your domain. In our example, we used cockroach.nyc as the domain:

Note that, for your A and CNAME records that point to your web server(s), the Status column should have an orange cloud with an arrow going through it. This indicates that the traffic will flow through CloudFlare’s reverse proxy before hitting your server(s).

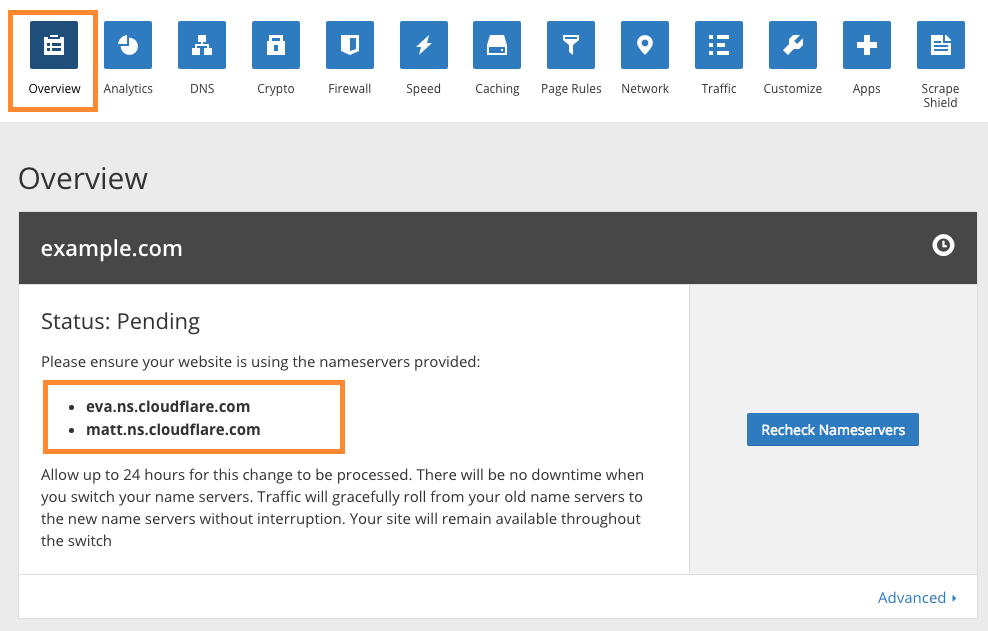


Next, select your CloudFlare plan.

**Change Your Nameservers**

For Godaddy users you can point your cloudflare nameservers from Godaddy by [following this process](http://www.slideshare.net/StanleyTan6/setting-up-cloudflare-for-go-daddy" \t "_blank).

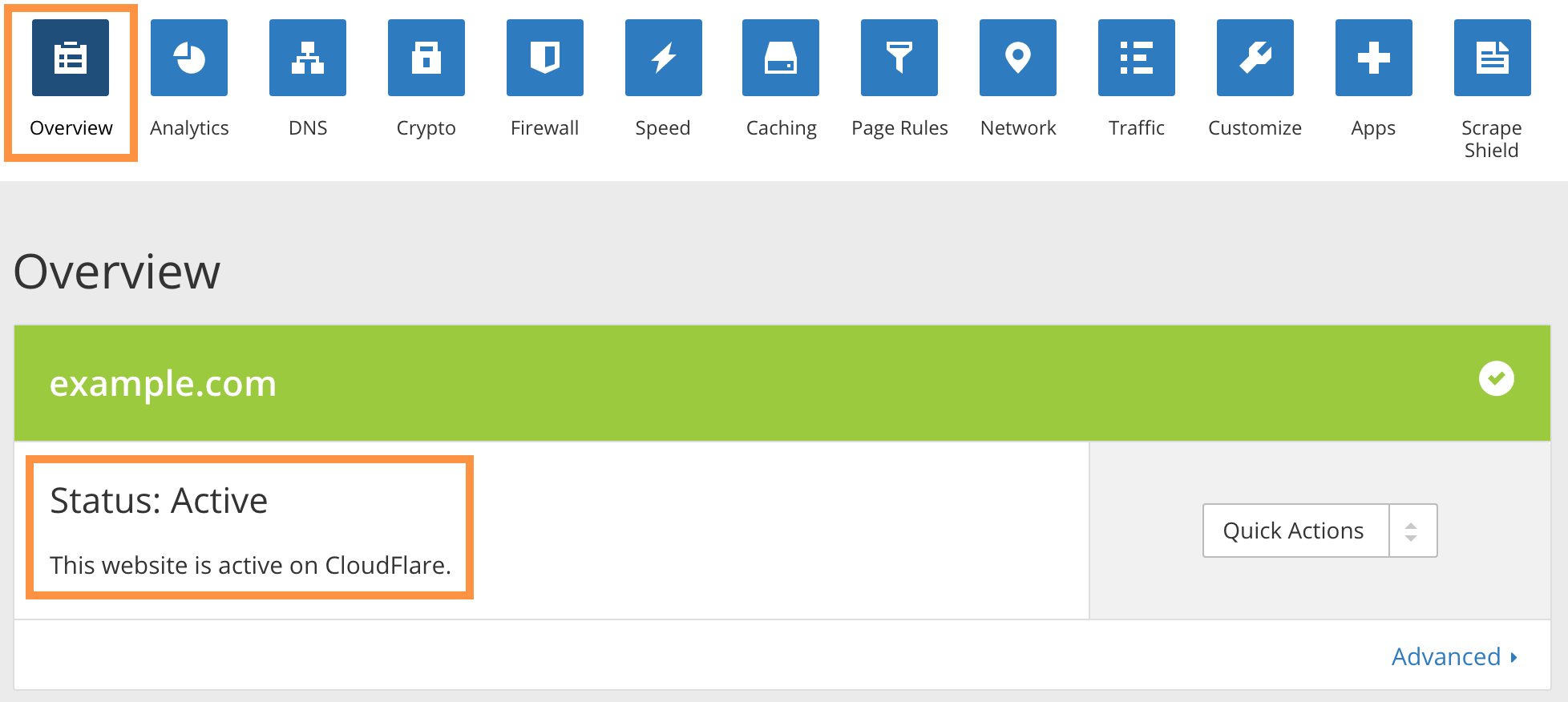
### Wait for Nameservers to Update



The Pending status means that CloudFlare is waiting for the nameservers to update to the ones that it prescribed (e.g. eva.ns.cloudflare.com and matt.ns.cloudflare.com). If you changed your domain’s nameservers, all you have to do is wait and check back later for an Active status. If you click theRecheck Nameservers button or navigate to the CloudFlare dashboard, it will check if the nameservers have updated.

### CloudFlare Is Active

Once the nameservers update, your domain will be using CloudFlare’s DNS and you will see it has anActive status, like this:



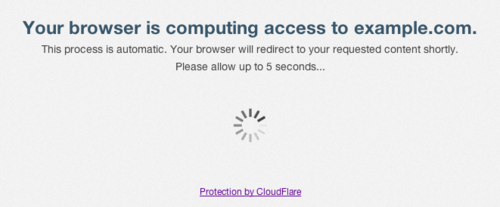
[Recommended First Steps for All CloudFlare Users](https://support.cloudflare.com/hc/en-us/articles/201897700). This is important to ensure that CloudFlare will allow legitimate connections from services that you want to allow, and so that your web server logs will show the original visitor IP addresses (instead of CloudFlare’s reverse proxy IP addresses).

Once you’re all set up, let’s take a look at the I’m Under Attack Mode setting in the CloudFlare firewall.

## I’m Under Attack Mode

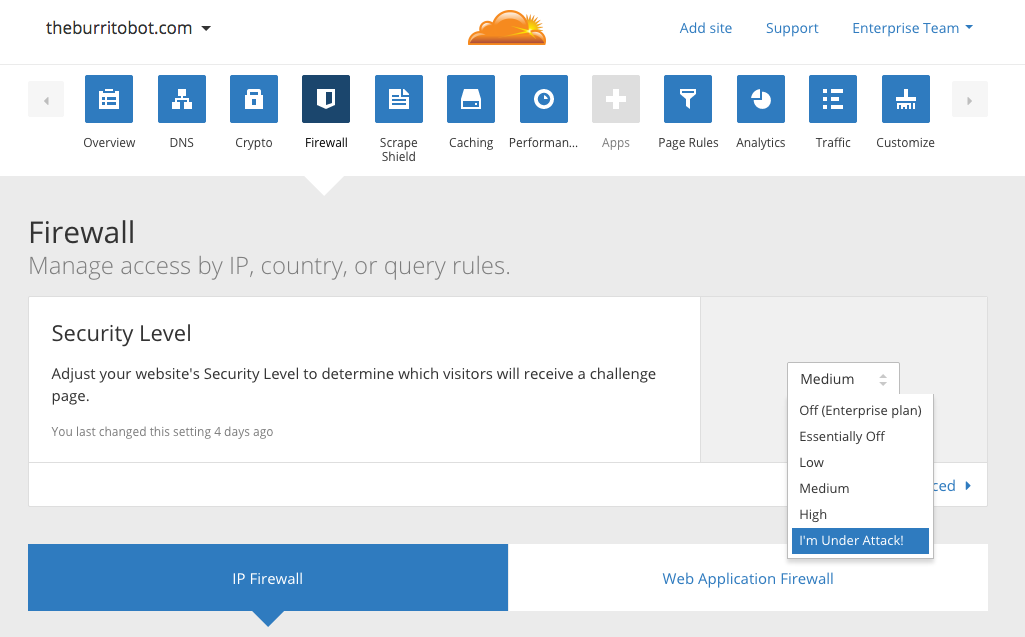
By default, CloudFlare’s firewall security is set to Medium. This offers some protection against visitors who are rated as a moderate threat by presenting them with a challenge page before allowing them to continue to your site. However, if your site is the target of a DDoS attack, that may not be enough to keep your site operational. In this case, the I’m Under Attack Mode might be appropriate for you.

If you enable this mode, any visitor to your website will be presented with an interstitial page that performs some browser checks and delays the visitor for about 5 seconds before passing them to your server.



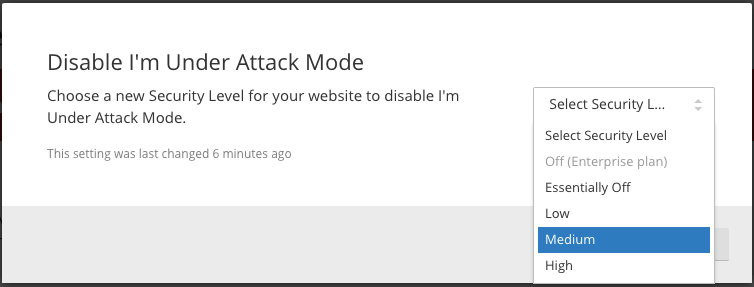
**Note:** Keep in mind that you only want to have I’m Under Attack Mode enabled when your site is the victim of a DDoS attack. Otherwise, it should be turned off so it does not delay normal users from accessing your website for no reason.

### How To Enable I’m Under Attack Mode



**How To Disable I’m Under Attack Mode**

As the I’m Under Attack Mode should only be used during DDoS emergencies, you should disable it if you aren’t under attack. To do so, go to the CloudFlare Overview page, and click the Disable button:



## Conclusion

Now that your website is using CloudFlare, you have another tool to easily protect it against HTTP-based DDoS attacks. There are also a variety of other tools that CloudFlare provides that you may be interested in setting up, like free SSL certificates. As such, it is recommended that you explore the options and see what is useful to you.

Good luck!

### Comments

# DDOS attacks and how to prevent them

Published Date : July 27, 2016  
Author : tayo



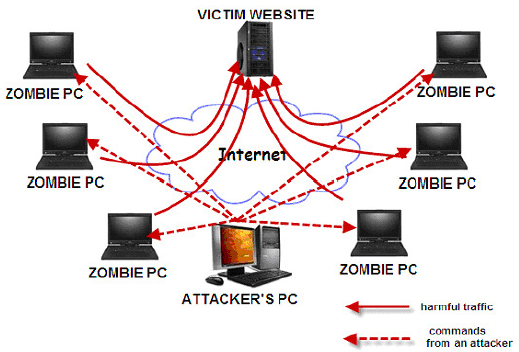
***There are several times more than the usual number of requests to connect to the site, but none of the computers where they’re coming from seem to exist. It’s like a distributed denial of service (DdoS) attack.***

Malicious users often disrupt web services with distributed denial of service (DDoS) attacks. These attacks send so much junk to a server that real traffic can’t get through. It’s a very old and effective technique that malicious users often employ to try and shut down a website.

**What is a DDoS attack?**

To understand a DDoS attack, we’ll talk about **denial of service** and **distributed denial of service attacks**. The main difference between the two is in the number of attackers. A denial of service (DOS) attack comes from one person or network, while a distributed denial of service attack (DDoS) uses many computers from networks all over the world. This amplifies the attack, and makes it harder for the target to protect itself.

**How a Denial of Service attack works**



Simply, a DOS floods a server with a huge amount of fake traffic, giving it far too many connection requests to handle, raising its bandwidth, tapping out its memory and eventually preventing real users from connecting to the server.

But even when a botnet uses many computers to open up a large number of connections, this is still quite hard to do. So, attackers can magnify the attack by using fake IP addresses. The attacking machine sends a connection request to the server using a fake IP address. The server responds and waits indefinitely for a further response – keeping the connection open – but none comes because the IP address was fake. The botnet repeats the process, making the server keep a lot of useless connections open and lose more and more memory until can’t cope any more and shuts down.

The strategy works and has slowed or crashed prominent websites. However, companies  have begun to take precautions.

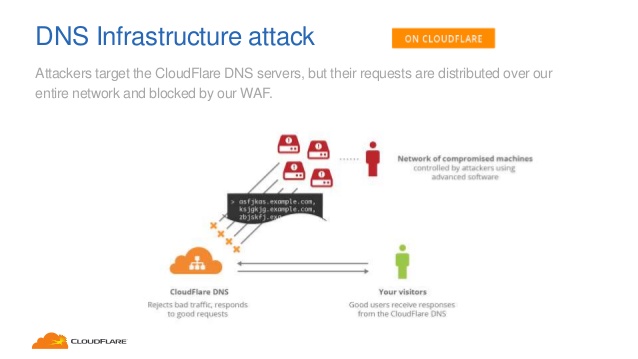
**Defending against a DDoS attack**

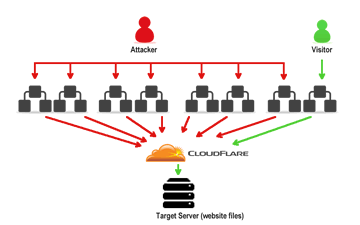
There are a few defences.

* **Filtering**: This works when routers on the network are programmed to detect and disconnect DDoS connections.



* **Moving defence**: which takes place when the target site’s IP address is changed if the attack is pointed at a particular IP address.
* **Blackholing**, or directing all traffic to a fake web address.
* The last is to simply use Content Delivery Networks (CDNs) like CloudFlare or Incapsula.





But nothing is guaranteed. So, the only definite way to end a DDoS attack is to wait for it to end, which it will. This is because of the people controlling botnets are online for too long during attacks, they can be detected and caught.

### Comments