

## Setting Up Barracuda Active DDoS Prevention

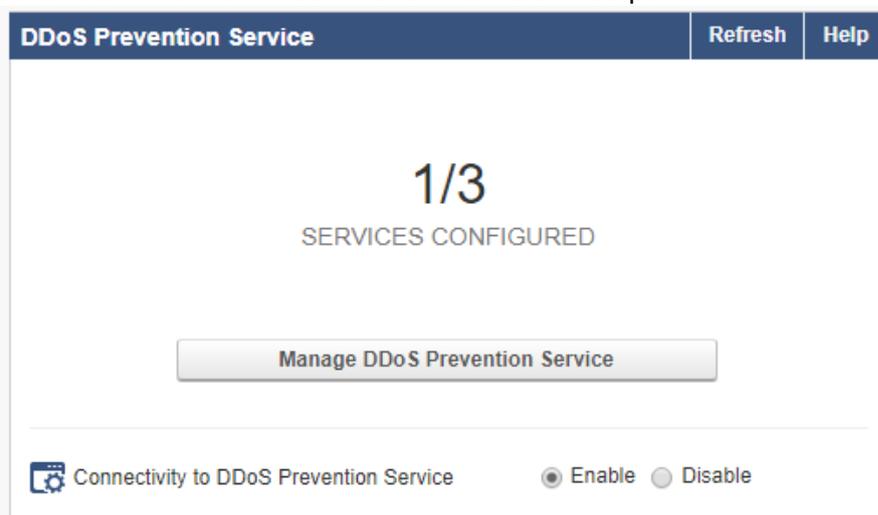
<https://campus.barracuda.com/doc/73700723/>

Follow these steps to set up Barracuda Active DDoS Prevention.

### A. Access the Barracuda Active DDoS Prevention Management Console

To access the Barracuda Active DDoS Prevention Management Console:

1. Log into the Barracuda Web Application Firewall and navigate to the **BASIC > Dashboard** page.
2. Scroll down to the **DDoS Prevention Service** pane.



3. For **Connectivity to DDoS Prevention Service**, select **Enable**. When prompted, confirm that you want to enable the connection. When you receive the success message, click **OK**.
4. In the DDoS Prevention Service pane, click **Manage DDoS Prevention Service**.

The **Web Application Firewall Services** page of Barracuda Active DDoS Prevention displays.

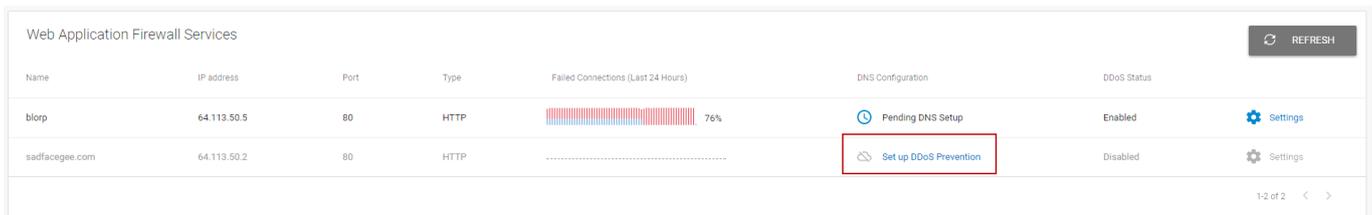
### B. Set Up DDoS Prevention

#### Note

For background information on the architecture of a service that uses the Barracuda Active DDoS Prevention, refer to [Understanding Service Architecture with Barracuda Active DDoS Prevention](#).

Before you begin:

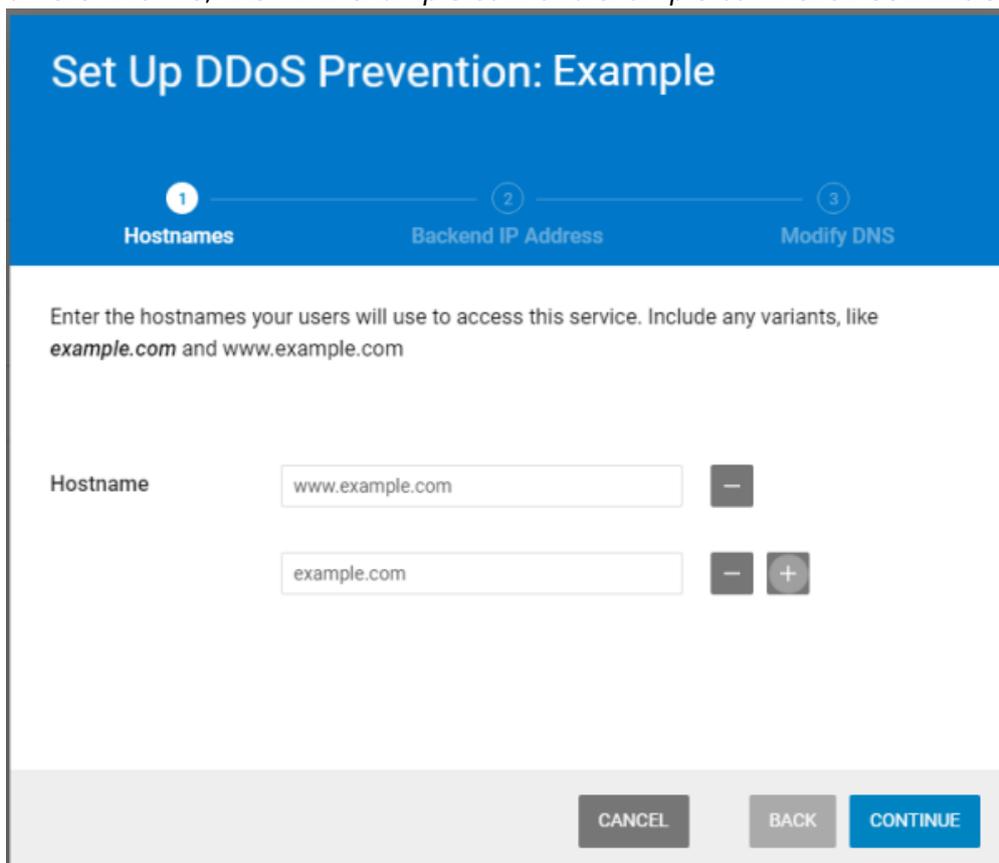
On the **Web Application Firewall Services** page of Barracuda Active DDoS Prevention, find the service you want to protect and click **Set Up DDoS Prevention**.



Name	IP address	Port	Type	Failed Connections (Last 24 Hours)	DNS Configuration	DDoS Status
blorp	64.113.50.5	80	HTTP	 76%	Pending DNS Setup	Enabled <a href="#">Settings</a>
sadfacegee.com	64.113.50.2	80	HTTP		<a href="#">Set up DDoS Prevention</a>	Disabled <a href="#">Settings</a>

To set up DDoS prevention on a service:

1. **Hostnames:** Enter all possible DNS domains your users will use to access this service, including different forms, like *www.example.com* and *example.com*. Click **Continue**.



## Set Up DDoS Prevention: Example

1 Hostnames      2 Backend IP Address      3 Modify DNS

Enter the hostnames your users will use to access this service. Include any variants, like *example.com* and *www.example.com*

Hostname  -

- +

CANCEL BACK CONTINUE

If one or more domains on a service have Barracuda Active DDoS Prevention configured, all domains on that service *must* also have it. All traffic will be blocked to any such domain without this configuration because all traffic to the service must pass through Barracuda Active DDoS Prevention. Note: the traffic will not be blocked until DNS records TTL (Time To Live) have had a chance to expire.

2. **Backend IP Address:** Enter the Backend IP Address for your service. This is typically the

Virtual IP Address defined for this service on your Web Application Firewall. Refer to [Understanding Service Architecture with Barracuda Active DDoS Prevention](#) for additional details.



3. Click **Test Connection** to ensure that Barracuda can connect to the Backend IP Address you specified.
  - If the test is successful, click **Continue**.
  - If you see a warning, refer to [Backend IP Address Errors](#) for troubleshooting information.
4. **Modify DNS**: Copy each line of information provided so you can change your DNS A records through your hosting provider. If you use the **Click to Copy** link, the new A record value is copied to your clipboard, so you can paste it directly into your service provider's interface in the next step. Click **Done**.

## Set Up DDoS Prevention: Example



### Change Your A Records

Visit your hosting provider's dashboard to change your A Records to the following, which hosting provider do you use? [Click here for more detailed instructions.](#)

**i** Changing your A Records causes no interruption or site downtime. The change can take up to 24 hours to take effect, but is not noticeable to you or your users.

Domain	Current A Record	Change A Record to
 www.example.com	93.184.216.34	64.113.50.7 <a href="#">Click to Copy</a>
 example.com	93.184.216.34	64.113.50.7 <a href="#">Click to Copy</a>

CANCEL

BACK

DONE

### Note

If you have more than one A record to change, you might want to keep this window open and open a new window for the next step, so you can copy between the two windows.

## C. Change A Records through your Domain Provider

Go to your domain provider's DNS management portal to change the A records you obtained in the previous step. Changing your DNS A records to point to your service's Service IP Address will redirect all of your web application traffic to Barracuda's Cloud Scrubbing Centers.

Reach out to your domain provider directly with any questions.

For your convenience, here is a list of popular domain provider knowledgebase entries to help you change your DNS A records.

- [GoDaddy](#)
- [NameCheap](#)
- [HostGator](#)
- [BlueHost](#)
- [1&1](#)

Note that these sites were current at time of publication and are not affiliated with Barracuda Networks.

You can also find the service IP Address in the Barracuda Active DDoS Prevention Management Console, by selecting **Settings** , then **Basic** .

## D. Change Origin IP

Change your IP range so historical DNS lookups do not expose your origin IP, allowing an attacker to bypass Barracuda Active DDoS Prevention. In addition, be sure you do not expose your origin IP in other DNS records, such as your MX (mail server) records.

Once you change your DNS records, traffic will automatically flow to the Barracuda Cloud Scrubbing Center. Remember that DNS records are public domain, and there are many places where historical records are archived. These historical DNS records will likely contain your original IP from before you activated Barracuda Active DDoS Protection. Therefore, Barracuda Networks recommends that once you activate Barracuda Active DDoS Protection, you change your IP range so a historical DNS lookup does not expose your origin IP. This could allow an attacker to bypass the Barracuda Cloud Scrubbing Center and attack your network infrastructure directly.

If you are using the Barracuda Email Security Gateway, you can use its Cloud Protection Layer feature to prevent your MX records from being exposed. Refer to [How to Set Up Your Cloud Protection Layer](#) in the Barracuda Email Security Gateway documentation for more information.

### Note:

IP addresses are sometimes removed from the "accept list." This is to prevent perpetrators that figure out the IP from flooding the original traffic destination. However, they will not be removed until the DNS TTL (Time To Live) has had a chance to expire, thus preventing traffic blocking for those using cached IPs.

## Figures

1. DDoSpane.png
2. WAFservices.png
3. 1.setup.png
4. 2.setupBackendIP.png
5. 3.changeArecords.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.