

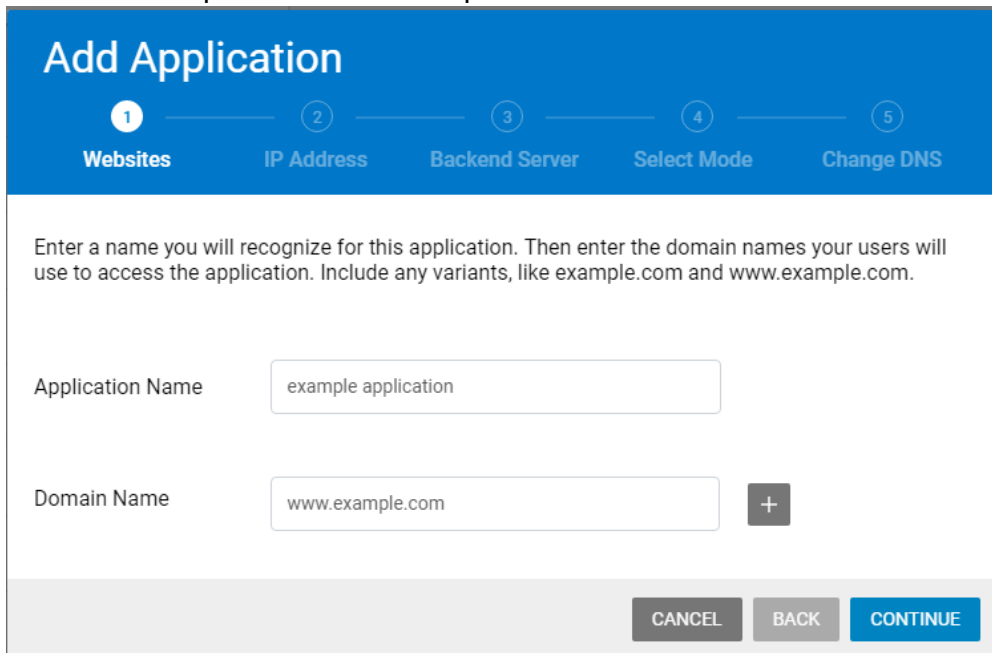
Getting Started

<https://campus.barracuda.com/doc/77399164/>

Follow these steps to configure Barracuda WAF-as-a-Service to protect your web applications. For an overview of the traffic flow you will have created through this process, refer to [Understanding Traffic Flow with Barracuda WAF-as-a-Service](#).

A. Configure Barracuda WAF-as-a-Service

1. Navigate to <https://waas.barracudanetworks.com/> and log in with your Barracuda account credentials.
If you do not already have a Barracuda account, click **Free 30-Day Trial** to sign up for a trial of WAF-as-a-Service.
2. At the top of the page, select **Applications**. Then click **Add Application**.
3. **Websites:** Enter a familiar name for the application you want to protect. Then 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**.



Add Application

1 Websites 2 IP Address 3 Backend Server 4 Select Mode 5 Change DNS

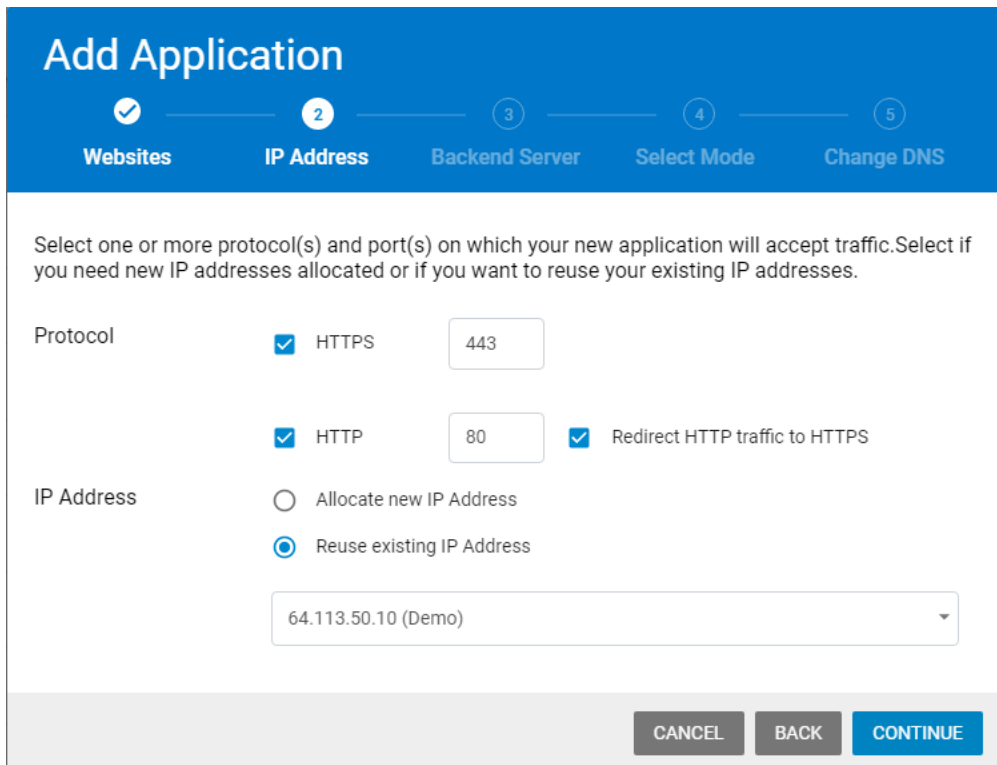
Enter a name you will recognize for this application. Then enter the domain names your users will use to access the application. Include any variants, like `example.com` and `www.example.com`.

Application Name

Domain Name +

CANCEL BACK CONTINUE

4. **IP Address:** Select one or more protocols and associated ports that Barracuda WAF-as-a-Service should listen on to protect your application. For HTTP traffic, you can choose if you want to add security by redirecting HTTP traffic to the more secure HTTPS protocol.
When you add your first application, you must allocate a new IP address for the application. For subsequent applications, you can choose to allocate a new IP address or reuse an IP address from an existing application. If you choose to reuse, select the IP address that you want to reuse. Refer to [IP Allocation](#) for more information. Click **Continue**.



Add Application

1 Websites 2 IP Address 3 Backend Server 4 Select Mode 5 Change DNS

Select one or more protocol(s) and port(s) on which your new application will accept traffic. Select if you need new IP addresses allocated or if you want to reuse your existing IP addresses.

Protocol

- HTTPS 443
- HTTP 80 Redirect HTTP traffic to HTTPS

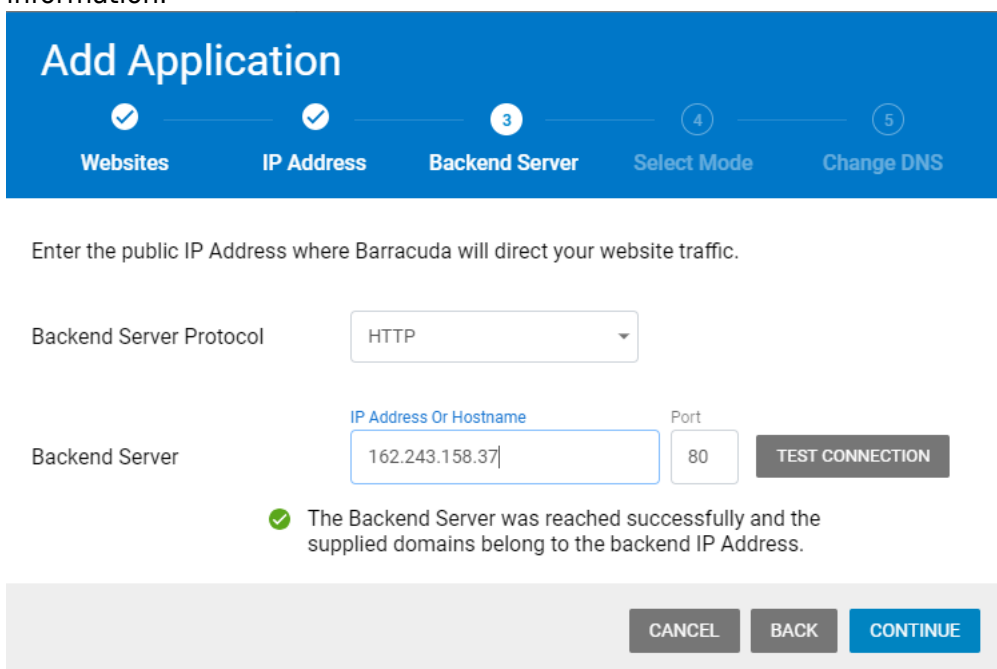
IP Address

- Allocate new IP Address
- Reuse existing IP Address

64.113.50.10 (Demo)

CANCEL BACK CONTINUE

- Backend Server:** Specify the protocol for the backend server – HTTP or HTTPS, then specify its IP address or Hostname and port. This is typically the current IP Address or hostname associated with the DNS domains you entered in step 1. Click **Test Connection** to ensure that Barracuda WAF-as-a-Service can connect to the backend server. When you have successfully tested the connection, click **Continue**. If the test displays a warning, refer to [Backend IP Address Errors](#) for troubleshooting information.



Add Application

1 Websites 2 IP Address 3 Backend Server 4 Select Mode 5 Change DNS

Enter the public IP Address where Barracuda will direct your website traffic.

Backend Server Protocol: HTTP

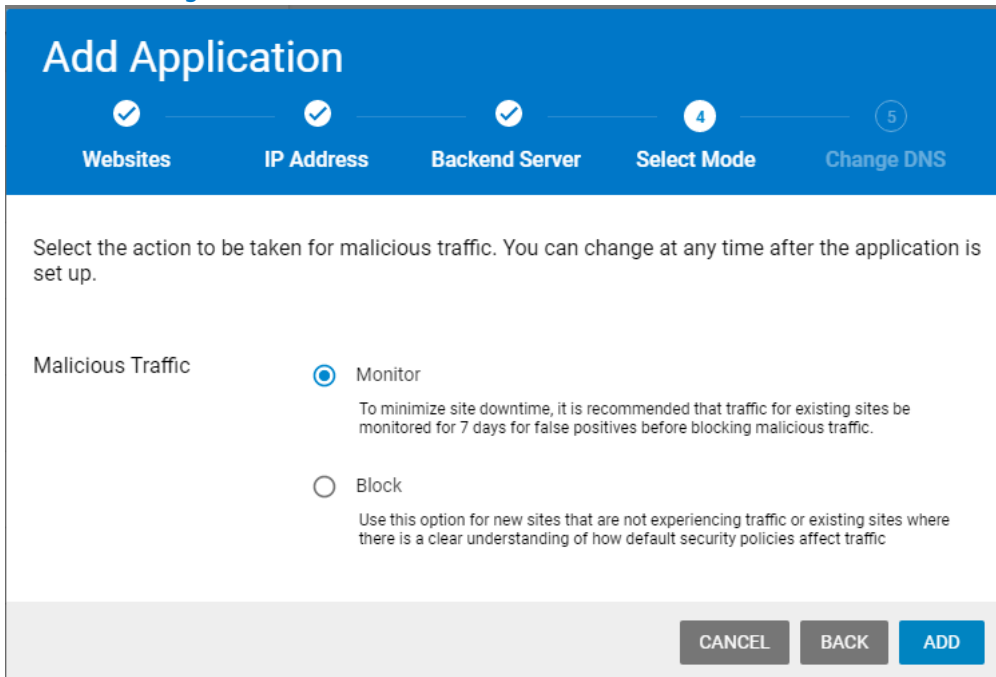
Backend Server: IP Address Or Hostname: 162.243.158.37 Port: 80 TEST CONNECTION

The Backend Server was reached successfully and the supplied domains belong to the backend IP Address.

CANCEL BACK CONTINUE

- Select Mode:** Specify whether you want to **Monitor** or **Block** malicious traffic. If you are

protecting an existing, live application, to minimize site downtime, we recommend you only monitor traffic for about a week before blocking malicious traffic. If you are protecting a new application, you can start blocking malicious traffic immediately. For more information, refer to [Understanding Monitor and Block Modes](#). Click **Add**.



Add Application

Progress: Websites ✓ IP Address ✓ Backend Server ✓ **Select Mode** 4 Change DNS 5

Select the action to be taken for malicious traffic. You can change at any time after the application is set up.

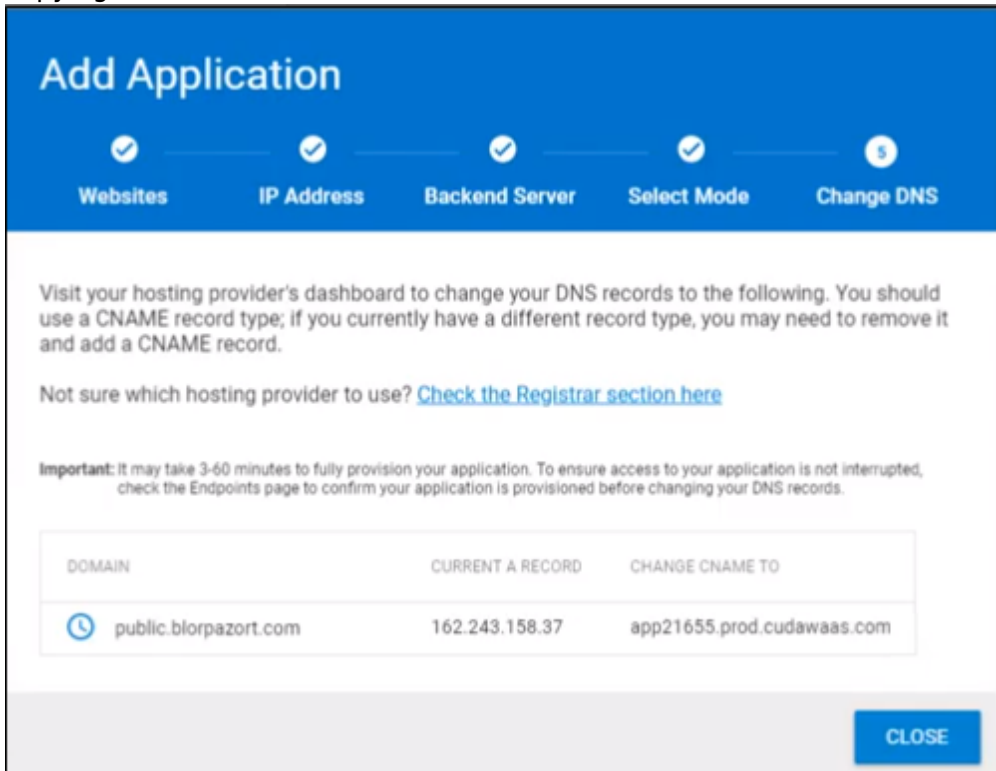
Malicious Traffic

Monitor
To minimize site downtime, it is recommended that traffic for existing sites be monitored for 7 days for false positives before blocking malicious traffic.

Block
Use this option for new sites that are not experiencing traffic or existing sites where there is a clear understanding of how default security policies affect traffic

CANCEL BACK ADD

7. **Change DNS:** Copy the CNAME domain provided so you can update your DNS records through your hosting provider. The CNAME is structured as `app#####.prod.cudawaas.com`. After copying the information, click **Close**.




Add Application

Progress: Websites ✓ IP Address ✓ Backend Server ✓ Select Mode ✓ **Change DNS** 5

Visit your hosting provider's dashboard to change your DNS records to the following. You should use a CNAME record type; if you currently have a different record type, you may need to remove it and add a CNAME record.

Not sure which hosting provider to use? [Check the Registrar section here](#)

Important: It may take 3-60 minutes to fully provision your application. To ensure access to your application is not interrupted, check the Endpoints page to confirm your application is provisioned before changing your DNS records.

DOMAIN	CURRENT A RECORD	CHANGE CNAME TO
 public.blorpazort.com	162.243.158.37	app21655.prod.cudawaas.com

CLOSE

Change DNS: Copy the 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 **Close**.

Add Application

Progress: Websites ✓ IP Address ✓ Backend Server ✓ Select Mode ✓ Change DNS 5

Visit your hosting provider's dashboard to change your A Record to the following. Not sure which hosting provider to use? [Check the Registrar section here](#)

Important: Changing your A records causes no interruption or site downtime. The change can take up to 24 hours, but is seamless for you and your users. interruption. Your site will remain available throughout the switch.

DOMAIN	CURRENT A RECORD	CHANGE A RECORD TO	
 www.example.com	93.184.216.34	64.113.50.64	CLICK TO COPY

[CLOSE](#)

Before You Continue...

To avoid downtime, wait until your application is completely provisioned before changing DNS information in Section B below.

Navigate to the [Endpoints](#) page for this application. On that page, a message displays while the new application is provisioning, a process that can take up to one hour. Wait until the message disappears, so you know the provisioning process is complete.

B. Add CNAME Records

Go to your domain provider's DNS management portal to add the CNAME record you created in the previous step. Adding the CNAME record will redirect all of your web application traffic to Barracuda WAF-as-a-Service. If you already have a CNAME record for your domain, edit the existing record. If you already have an A record for your domain, delete the A record first, then create the CNAME record.

Reach out to your domain provider directly with any questions.

Change A Records

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 application's IP Address will redirect all of your web application traffic to Barracuda WAF-as-a-Service.

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 records.

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

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

C. Restrict Direct Traffic

Ensure that users cannot access your application server directly, without going through Barracuda WAF-as-a-Service. For full instructions, refer to [Restricting Direct Traffic](#).

D. Change Origin IP

Change your IP range so historical DNS lookups do not expose your origin IP, allowing an attacker to bypass Barracuda WAF-as-a-Service. In addition, be sure not to expose your origin IP in other DNS

records, such as your MX (mail server) records.

After you change your DNS records, traffic will automatically flow to Barracuda WAF-as-a-Service. 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 WAF-as-a-Service. Therefore, Barracuda recommends that after you activate Barracuda WAF-as-a-Service, you change your IP range so a historical DNS lookup does not expose your origin IP. Having that information could allow an attacker to bypass Barracuda WAF-as-a-Service 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.

Figures

1. addApp.png
2. AddApplication2.png
3. image2018-5-15 13:21:44.png
4. AddApplication4.png
5. copyCNAME.png
6. AddApplication5.png

© Barracuda Networks Inc., 2020 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.