Restricting Direct Traffic

https://campus.barracuda.com/doc/77401091/

After you set up Barracuda WAF-as-a-Service for one or more of your applications, ensure that users cannot access your application server directly, without going through Barracuda WAF-as-a-Service.

Be sure to follow these procedures if you change the deployment location of your applications. For details, refer to Moving an Application to Another Location.

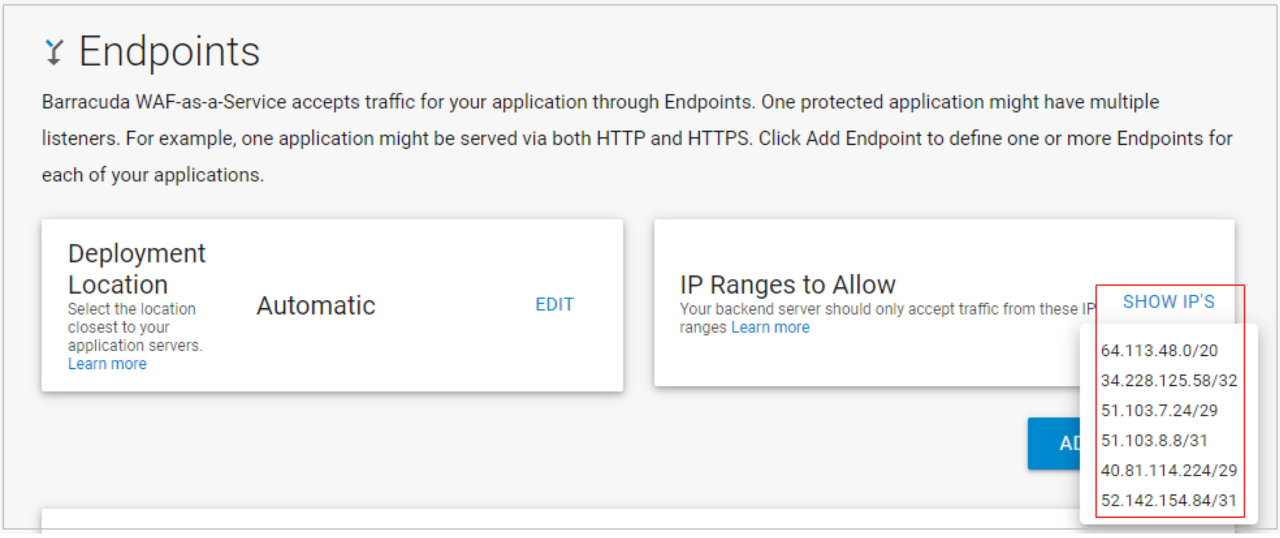
Restricting Direct Traffic

For accounts created on or after November 5, 2019

Barracuda WAF-as-a-Service provides the IP ranges you need to accept.

To locate the IP ranges:

1. Log into Barracuda WAF-as-a-Service and navigate to **Applications**.
2. Click the application name.
3. In the left panel, select **Endpoints**.
4. On the **Endpoints** page, locate the **IP Ranges to Allow** section. Click **Show IPs**, then copy the IP ranges listed.



Endpoints

Barracuda WAF-as-a-Service accepts traffic for your application through Endpoints. One protected application might have multiple listeners. For example, one application might be served via both HTTP and HTTPS. Click Add Endpoint to define one or more Endpoints for each of your applications.

Deployment Location
Select the location closest to your application servers. Learn more

Automatic

IP Ranges to Allow
Your backend server should only accept traffic from these IP ranges Learn more

64.113.48.0/20
34.228.125.58/32
51.103.7.24/29
51.103.8.8/31
40.81.114.224/29
52.142.154.84/31

5. Configure your backend server to accept traffic only from those IP ranges. See sections below for guidance.

For accounts created before November 5, 2019

Configure your application server to accept traffic only from the following Barracuda IP ranges.

- `64.113.48.0/20`
- `34.228.125.58/32`
- `51.103.8.8/31`
- `52.142.154.84/31`

Note: The IP address 34.228.125.58 is used in the Test Connection step of adding an application. For details, refer to Getting Started.

Allowing IPs for Exporting Logs

To export your log information, as described in Log Export, now is a good time to allow those IPs as well.

To export logs, be sure to allow the following IPs:

- `34.227.174.172`
- `40.71.30.40`

Note: If you deploy Barracuda WAF-as-a-Service in your own containers and choose to export logs directly from your containers, these IP addresses do not apply. Make sure the containers you deploy have access to your log servers.

Configuring Your Backend Server

Consult your backend server documentation for specific instructions on this process. Here are links to some backend server documentation sets.

Application Servers

- Apache HTTP Server
- Microsoft IIS webserver

- Nginx Web Server

Host-Based Network Firewall

- Microsoft Windows Defender Firewall
- Unix and Linux Iptables

Cloud-Based Networks and Firewalls

- Barracuda CloudGen Firewall Access Rules
- Microsoft Azure Network Security Groups
- Amazon Web Services Security Groups
- Google Cloud Platform VPC Firewall Rules

Figures

1. endpointsShow2.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.