IP Reputation-Based Filters

https://campus.barracuda.com/doc/4259852/

Overview

In order to prevent geographically distributed DoS attacks that span multiple subnetworks, the Barracuda Web Application Firewall provides an IP reputation-based filter that can be applied to an entire geographic region or collection of regions spanning multiple countries and/or continents.

This feature is available only in firmware version 7.7 or higher.

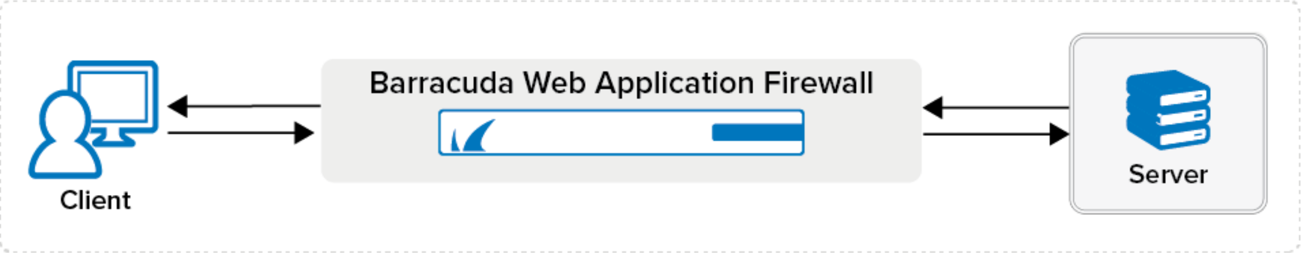
You can configure a geo pool with one or more geographic regions and allow or deny requests from it. IP addresses can be filtered based on the following categories:

- **Geo Pool** – The IP address is from an included geographic region.
- **Barracuda Reputation Blocklist** – The IP addresses that are identified as potential originators of spam, malware, and bots.
- **TOR Nodes** – The IP addresses that are identified as TOR.
- **Anonymous Proxy** – The IP address is from an anonymizer that hides the IP address of the requesting client.
- **Satellite Provider** – The IP address is from a Satellite Internet Service Provider (ISP) so the IP address of the requesting client is unknown.
- **Public Proxy** – The IP address of a public proxy server that hides the IP address of the actual client and allows access to the web application.
- **Known HTTP Attack Sources** – The IP addresses that scan HTTP/HTTPS requests for vulnerable installations of known web applications and brute force logins.
- **Known SSH Attack Sources** – The IP addresses that run attacks on the service SSH.
- **Datacenter IP** – The IP address is from a range of data centers and is therefore not the user but rather a program.
- **Fake Crawlers** – The IP addresses of robots that crawl the web application by sending user-agent strings of reputed/popular search engines such as Google, Bing, Yandex, etc.

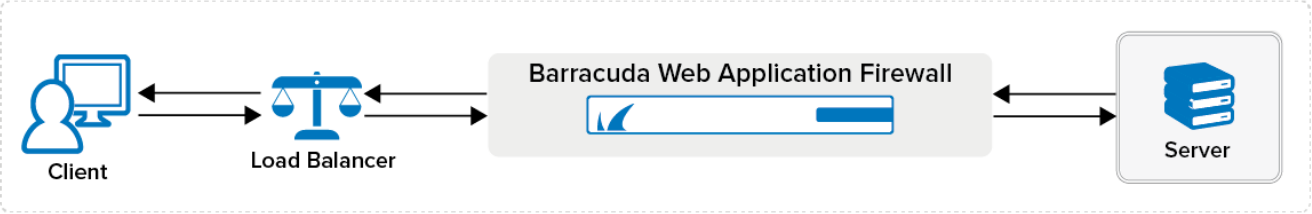
Anonymous Proxy and Satellite Provider IP addresses are not specific to geographic regions. IP addresses are compared to the MaxMind database to determine if the requester is a known anonymizer or ISP address.

Once a geo pool is created, it can be associated with one or more services using the **IP Reputation Filter** section on the **WEBSITES > IP Reputation** page.

An IP Reputation Filter policy can be applied at the **Network Layer** or **Application Layer**. When set to **Network Layer**, the Barracuda Web Application Firewall applies the IP Reputation policy at the network layer. In this case, the socket IP address that is used to establish the connection with the service IP address of the Barracuda Web Application Firewall is used as the client IP address. Use **Network Layer** when the Barracuda Web Application Firewall is deployed directly between the client and the server, without any intermediate device like a load balancer deployed between the client and the Barracuda Web Application Firewall. In this scenario, clients establish a direct connection with the Barracuda Web Application Firewall to send requests. Any request sent by the client is received directly by the Barracuda Web Application Firewall.



If the clients connect to the Barracuda Web Application Firewall through an intermediate device such as a load balancer, the connection is established by the intermediate device instead of the actual client. In such cases, the Barracuda Web Application Firewall cannot identify the client's IP address at the network layer. It is recommended to use the **Application Layer** IP Reputation policy when there is an intermediate device between the client and the Barracuda Web Application Firewall. When set to **Application Layer**, the Barracuda Web Application Firewall uses the client IP address from the HTTP request header (e.g. **X-Forwarded-For** header) to identify the actual client IP address and applies the IP Reputation policy.



Geographic Filtering

You can create a geo pool on the **WEBSITES > IP Reputation** page, in the **Add Geo Pool** section.

Create a New Geo Pool

1. Enter a name for the pool in **New Geo Pool Name**.

> The name can include alphanumeric characters, periods (.), hyphens (-) and underscores (_). Any other special characters such as space, semicolon, asterisk, etc. are not allowed.

2. Select the geographic region(s) to include in your IP Reputation Filter using the **Expand** button. Expand lists smaller regions inside a continent, and Collapse lists discrete continents. When you can discretely select the areas you desire, select one or more entities you wish to geographically filter. Alternatively, you can use **Select All** or **Deselect All**.
3. Click **Add** to save the new geo pool. The created pool appears in the **Geo Pools** list showing the configured settings.

Use the **Geo Pools** section to edit or delete an existing geo pool.

- To Edit: Select the **Edit** icon from the Options column next to the desired geo pool.
- To Delete: Select the **Delete** icon from the Options column next to the geo pool you wish to delete.

Click **Help** on the relevant page for more information.

You must associate the newly created geo pool to a service to enable filtering for the selected geographic region. See Applying an IP Reputation Filter to a Service.

Blocking the IP Address(es) Using the Custom IP List

The Custom IP list is a text file that contains a list of block-listed IPs. This text file can be bound to a service. When a client accesses a service, and if the IP address of the service is listed in the Custom IP list text file, the Barracuda Web Application Firewall will block the IP address.

You can upload/download a Custom IP list text file to the Barracuda Web Application Firewall.

Applying an IP Reputation Filter to a Service

To associate a geo pool to a service, perform the following steps:

1. Go to the **WEBSITES > IP Reputation > IP Reputation Filter** section.
2. Identify the service to which you want to associate a geo pool. Click **Edit** next to it. The **Edit IP Reputation Filter** window appears.
3. In the **IP Reputation Filter** section:
   1. Set **Enable IP Reputation Filter** to *On* to enable the filter for the service.
   2. Set **Enable Logging** to **Yes** if you want to generate logs for the IP reputation policy. If **Apply Policy at** is set to **Network Layer** and **Enable Logging** is set to **Yes**, the logs

can be viewed on the **NETWORKS > Network Firewall Logs** page. When **Apply Policy at** is set to **Application Layer**, the logs can be viewed on the **BASIC > Web Firewall Logs** page.

> **Enable Logging** is applicable only for Network Layer.

4. In the **Geo IP Filter** section, set the **Action** to *Allow* or *Block*:
    - **Allow** – Allows the traffic only from the selected geographical regions, but blocks the traffic from other geographical regions.
    - **Block** – Blocks the traffic only from the selected geographical regions, but allows the traffic from other geographical regions.
5. In the **Block IP Categories** section, select the IP categories that need to be blocked for this service. When set to **Block**, the requests from the IP addresses of the selected category will be terminated and logged. You can override any of these IP address(es) and allow by adding the IP address(es) in **Allowed Networks** in the **Exception Networks** section.
    - **Barracuda Reputation Blocklist** – Set to **Block** to block the IP addresses that have been identified as potential originators of spam, malware, and bots. When **Apply IP Reputation Policy** is set to **Network Layer**, the Barracuda Web Application Firewall communicates with the local database stored in the system to validate the requests. If **Apply IP Reputation Policy** is set to **Application Layer**, the Barracuda Web Application Firewall communicates with **Global Real Time IP Look UP (GRIP)**, a cloud service that contains IP addresses that have been identified as potential originators of spam, malware, and bots by Barracuda’s threat intelligence engine.
    - **TOR Nodes** – Set to **Block** to block the IP addresses that have been identified as TOR.
    - **Anonymous Proxy** – Set to **Block** to block the IP addresses that are used as anonymizers to hide the identity of the client's IP address.
    - **Satellite Provider** – Set to **Block** to block the IP addresses from the Satellite Internet Service Providers (ISPs) that provide internet service.
    - **Custom IP List**– Set to **Block** to block the IP addresses in the **Custom Blocklist File**.
    - **Public Proxy** - Set to **Block** to block the IP addresses from public proxies.
    - **Known HTTP Attack Sources** - Set to **Block** to block the IP addresses from known HTTP attack sources.
    - **Known SSH Attack Sources** - Set to **Block** to block the IP addresses from known SSH attack sources.
    - **DataCenter IP** - Set to **Block** to block the IP addresses from known datacenters.
    - **Fake Crawler** - Set to **Block** to block the IP addresses from known fake crawlers.

    > Blocking the IP addresses as listed in the Custom IP List text file by the Barracuda Web Application Firewall is applicable only for Network Layer IP Reputation.
6. In the **Block ASNs** section, select the ASN group for which you want to block or allow traffic. If **Action** is set to **Block**, traffic from all AS numbers listed in the selected ASN group is blocked. If set to **Allow**, traffic from all AS numbers listed in the selected ASN group is allowed, but the traffic from other AS numbers is blocked.
7. In the **Exception Networks** section, enter the IP address(es) that needs to be considered an exception despite originating from the geographical region specified in the geo pool, or from the Block IP Categories.
    - **Allowed Networks** - Enter the IP address(es) and associated subnet mask that needs to be allowed in spite of getting matched with the configured Geo IP rules or Block IP Categories rules.

    - **Blocked Networks** - Enter the IP address(es) and associated subnet mask that needs to be blocked in spite of getting matched with the configured Geo IP rules or Block IP Categories rules.

8. Click **Save**. The configured IP Reputation Filter will now be applied to all requests for the service.

Click **Help** on the relevant page for more information.

Upload a Custom IP List Text File

1. Click the **Upload** option from the **Custom IP List** field.
2. Click **Browse** and select the text file that contains the list of block-listed IPs. The URL of the selected text file is listed in the **Upload File Of Blocklisted IPs** text box.
3. Click **Upload Now** to upload the text file to the Barracuda Web Application Firewall.

- When a new Custom IP list is uploaded, it overwrites the old list.
- Currently, there is no restriction to the number of IP addresses that can be included in the Custom IP list; however, having a large number of IP addresses can reduce the performance.
- CIDR is not supported.

Download a Custom IP List Text File

1. Click the **Download** option from the **Custom IP List** field.
2. In the **Download URL** text box, enter the URL of the text file present on the server.

   The URL of the Custom IP List does not support HTTP.
3. Select **Yes** from the **Validate Server Certificate** field to validate the server certificate.
4. Click the **Trusted Certificate** drop-down list and select the certificate that must be validated against the server.
5. Click **Download**. The text file that contains the list of block-listed IP addresses is downloaded to the Barracuda Web Application Firewall.

Figures

© 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.