How to Configure Trusted Hosts

Trusted Hosts

The Barracuda Web Application Firewall allows you to designate Trusted Hosts by IP address and Mask which are not subjected to security checks. Traffic coming from trusted hosts is assumed to be safe. The **WEBSITES > Trusted Hosts** page allows you to create a trusted hosts group with one or more hosts. Trusted Host Groups have an associated **Trusted Hosts Action** so a policy violation from a Trusted Host results in the **Trusted Hosts Action** overriding the **Action** configured for other hosts. You can set the **Trusted Hosts Action** to:

- *Allow* - All requests pass through, including possible attacks (which are ignored); No logs are generated.
- *Passive* - All requests pass through, including possible attacks, but logs are generated on the **BASIC > Web Firewall Logs** page.
- *Default* - Trusted hosts are treated the same as all other clients.

Steps to create a trusted hosts group:

1. Go to the **WEBSITES > Trusted Hosts** page.
2. In the **Add New Trusted Host** section, specify a name in the **Trusted Hosts Group Name** field and click **Add**.
3. In the **Trusted Hosts** section, click **Add Host** next to the **Trusted Host Group** that you created. The **Create Trusted Host** window appears. Specify values for the following:
    1. **Trusted Host Name** – Enter a trusted host name to which you want to exempt the security checks. Host names cannot include space characters.
    2. **Version** – Select the Internet Protocol version (IPv4 or IPv6) for the trusted host from the drop-down list.
    3. **IP Address** – Enter the IP address of the trusted host.
    4. **Mask** – Enter the netmask associated with the IP address.
4. Click **Add**.
5. If you wish to add multiple hosts to the Trusted Hosts group, repeat **Step 3** and **Step 4**.

Associate a Trusted Hosts Group with a Service

Once a trusted hosts group is created with a set of trusted hosts, you can associate that group to a Service and exempt them from security checks or authentication as explained below.

Exempting a Trusted Hosts Group from Security Checks

The following steps bind a trusted hosts group with a Service and exempts them from security checks.

1. Go to the **BASIC > Services** page.
2. In the **Services** section identify the Service to which you want to associate the trusted hosts group for exempting security checks.
3. Click **Edit** next to the Service. The **Service** window appears.
4. Scroll down to the **Basic Security** section and set **Trusted Hosts Action** to *Allow* or *Passive*.
5. Select the **Trusted Hosts Group** from the drop-down list.
6. Specify values to other parameters as required and click **Save**.

Exempting a Trusted Hosts Group from Authentication

If you do not wish to require authentication for a set of trusted hosts, associate the trusted hosts group with an authentication policy and set the **Trusted Hosts Action** to *Allow*. The Barracuda Web Application Firewall identifies the trusted hosts as allowed users and all of its requests are exempted from authentication.

Steps to associate a trusted host group with an authentication policy:

1. Go to the **ACCESS CONTROL > Authentication** page.
2. In the **Authentication Policies** section, identify the Service to which you want to associate the trusted host group that you are exempting from authentication.
3. Click **Edit** next to that Service. The **Edit Authentication Policy** window appears.
4. In the **Edit Authentication Policy** window, select the **Trusted Hosts Group** from the drop-down list to associate it with the policy.
5. Set **Trusted Hosts Action** to *Allow* to exempt the set of trusted hosts from authentication.
6. Specify values to other parameters as required and click **Save**.

Learning from the Trusted Hosts

When a Service is associated with a security policy, all URLs and Parameters are matched to that security policy setting. Web applications are dynamic and vary widely, so a one size fits all security strategy might not be adequate across a website. For this reason, it might block some genuine requests which are identified as false positives. You can reduce false positives and fine tune the security settings for a trusted hosts group using one of the following:

- Adaptive Profiling
- Exception Profiling

Both assist in development of fine grained security settings. Exception Profiling uses a heuristics based strategy to refine web application security settings in response to logged traffic on **BASIC > Web Firewall Logs**. Adaptive Profiling learns the intricate structure of an application and enforces conformance to it. Detailed security profiles are created by Learning from requests and responses served by a particular web application. For more information on how exception profiling works, see How to Configure Exception Profiling.

Fine Tuning Security Settings for a Trusted Hosts Group using Adaptive Profiling

1. Go to the **WEBSITES > Adaptive Profiling** page.
2. Click **Edit** next to the Service to which you want to associate a trusted host group and learn the requests and/or responses from the trusted hosts. The **Edit Service Adaptive Profiling** window appears.
3. Select *Trusted* from the **Request Learning** drop-down list if you wish to learn the requests from a trusted host.
4. Select *Trusted* from **Response Learning** drop-down list if you wish to learn the responses from a trusted host.
5. Select **Trusted Hosts Group** from the drop-down list.
6. Specify values to other parameters as required and click **Save**.

Fine Tuning Security Settings for a Trusted Hosts Group using Exception Profiling

1. From the **WEBSITES > Exception Profiling** page identify the Service to which you want to bind the trusted hosts group.
2. Click **Edit** next to that Service. The **Edit Exception Profiling** window appears.
3. Select **Trusted Hosts Group** from the drop-down list.
4. Set **Learn From Trusted Hosts Group** to *Yes* and click **Save**.
5. The exceptions from trusted hosts are learned using trusted hosts heuristics displayed on the **WEBSITES > Exception Heuristics** page.
6. Select **Exception Profiling Level** from the drop-down list if you wish to learn from non-trusted hosts as well. The exceptions from non-trusted hosts are learned based on Low, Medium or High exception profiling settings on **WEBSITES > Exception Heuristics**.