Configuring and Deploying a Firewall using AWS

https://campus.barracuda.com/doc/90440464/

Before You Begin

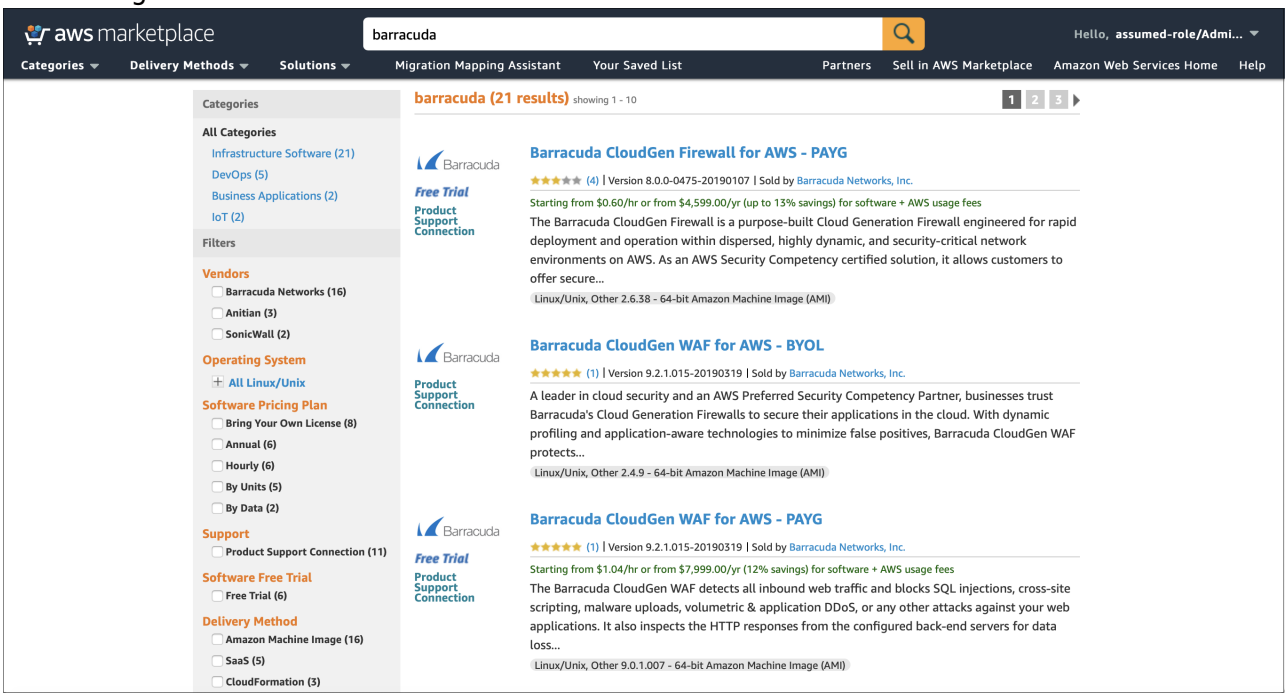
Update Permissions for Existing AWS Cloud Accounts

You might need to update permissions for existing AWS cloud accounts that you already added to Barracuda Cloud Security Guardian. Follow the instructions in Updating the Cloud Formation Template in AWS.

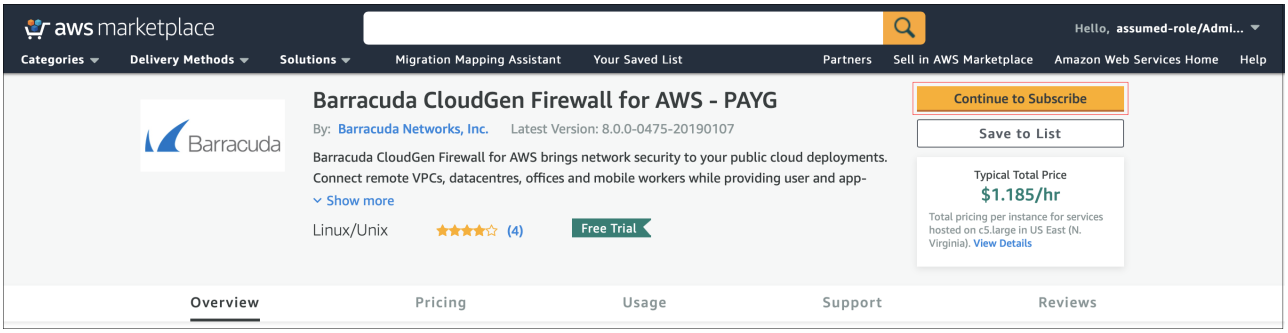
Agree to the Terms of Service

To deploy a CloudGen Firewall image template, you must agree to the Terms of Service and subscribe to the image in the AWS Marketplace. You need to do this only once per account, you must do this separately for PAYG and BYOL images.

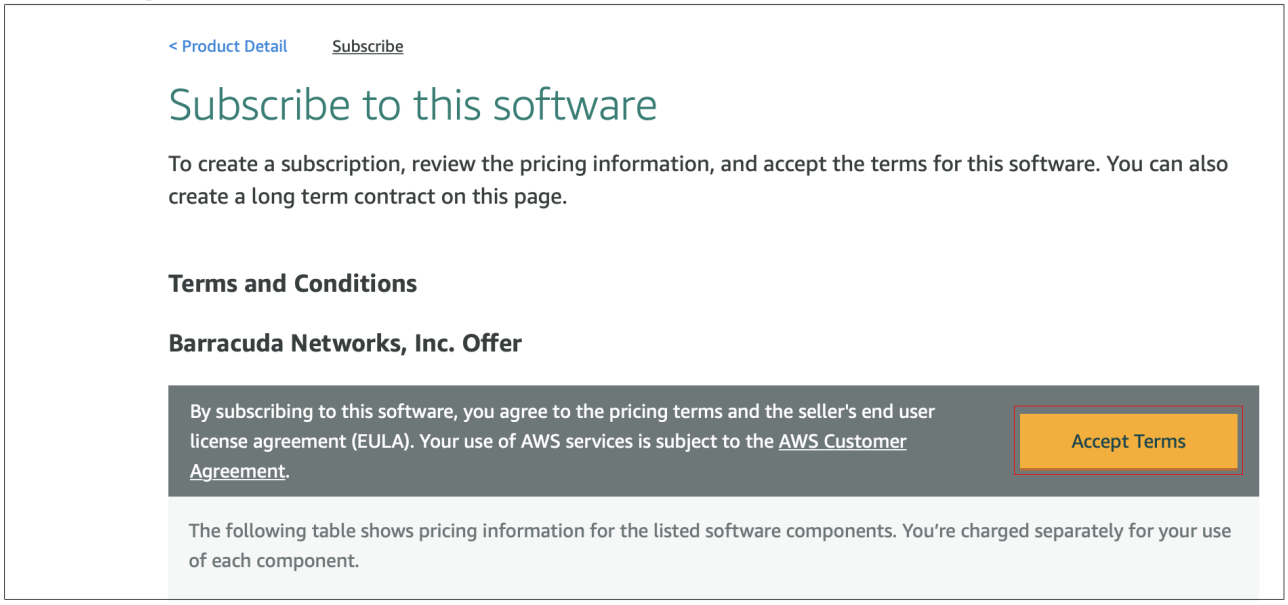
1. Go to the AWS Marketplace: https://aws.amazon.com/marketplace/.
2. Search for `Barracuda CloudGen Firewall`.
3. Click on the Barracuda CloudGen Firewall PAYG or Barracuda CloudGen Firewall F-Series BYOL image.



4. Click **Continue**.



5. Click **Accept Terms**.



You will now receive an email from Amazon confirming your subscription. You can now use the provided AMI in your CloudFormation templates.

Step 1: Create a Shared Firewall Policy

A Shared Policy is a way of grouping firewalls together.

New accounts do not have any Shared Policies, so the Shared Firewall Policies page is blank.

To create a new Shared Policy:

1. Log into your Barracuda Cloud Security Guardian account.
2. From the menu, navigate to **Policy Management > Infrastructure**.
3. On the Infrastructure Policies page, click **Add Shared Policy**.
4. Enter a Name for this Shared Policy and click **Add**.
   The new Shared Policy appears in the **Shared Firewall Policies** list.

You can edit or delete the Shared Policy at any time. Click the three dots in the table and select the appropriate action.

- **Editing** the Shared Policy enables you to change the Policy's name within Barracuda Cloud Security Guardian.
- **Deleting** the Shared Policy removes it from your instance of the Barracuda Cloud Security Guardian. The Delete option is only available for Policies that do not contain any Firewalls.

Step 2: Deploy a Firewall

1. Click **Deploy Firewall**.
2. For the Group, select the Shared Policy you just created.
   Alternatively, you can enter a name to create a new group here.
3. Click **Next** to continue.
4. Provide a name for the new Firewall Instance. This should be a fairly specific name.
5. Optionally create a description for the Firewall. Click **Next** to continue.
6. Select the Location for your Cloud Service Provider – here, AWS. The list of Regions in that Location loads automatically.
7. Select the Region where you want to deploy the Firewall. For example, `US-West` or `EU-North`. Click **Next** to continue.
8. Select the Barracuda CloudGen Firewall. The window expands to display all of the required fields. Enter the following information:
   - **New/Existing VPC** – Select whether you are deploying to a new VPC or to an existing VPC.
     - **For a New VPC** – In the **VPC Address Space**, specify the subnet in CIDR notation. For example, `10.0.0.0/8`.
     - **For an Existing VPC** – Select the existing VPC from the list of available VPCs for the region you specified in Step 7 above.
   - **MIP1** – Enter an IP address within the VPC Address Space you specified above.
   - **MIP2** – Enter a second IP address within the VPC Address Space you specified above.
   - **Availability Zone 1** –Select an Availability Zone from within the Region specified earlier.
   - **Availability Zone 2** – Select a second Availability Zone from within the Region specified earlier.
   - **Instance Type** – Select the size and pricing structure for this instance.
   - **Admin Password** – Create and confirm a password to be used by the Firewall Administrator.
   - **Admin Email** – Specify the email address for communicating with the Firewall Administrator.
9. Click **Next** to continue.
10. Click **Deploy**. The Infrastructure Policies page displays with the new firewall in the Shared Policy Group you specified. Refresh the page, if needed.
    The Barracuda CloudGen Firewall is configured and deployed, changing states from **Deploying** to **Ready**.
    When the new firewall is ready, it is listed under the appropriate Group/Shared Policy. You can access it with the login you created.

Step 3: Create Rules

After the new firewall is ready, you can create rules at the Group/Shared Policy level or at the local

level for a single firewall. Learn more about the Barracuda CloudGen Firewall.

Newly created rules must synchronize with the firewall. This process can take approximately ten minutes to complete.

Group/Shared Policy Rules

To create shared rules:

1. In the Shared Firewall Policies list, locate the Shared Policy for which you want to create rules. In its table row, click **Rules**.
2. Select the appropriate tab to create either **Layer 4 Rules** or **Domain Rules**. Click **Add Rule**.
   Layer 4 Rules – Creates inbound and outbound layer 4 network rules, for example which IP addresses are able to access which destination IP addresses.
   Specify the following information, then click **Add**.
   - **Name** – Specify a unique name for this new rule.
   - **Protocol** –Select the protocol to use for this rule: **TCP**, **UDP**, or **Any**.
   - **Action** – Select the type of rule, **Allow** or **Block**.
   - **Features** – Select either one or both: **IPS/IDS**, **Application Control**. If you choose **IDS/IPS**, you can only deploy the rule set on a Barracuda CloudGen Firewall.
   - **Source IP Address** – Provide the Source IP Address.
   - **Destination IP Address** – Provide the Destination IP Address.
   - **Port** – Provide the Port.

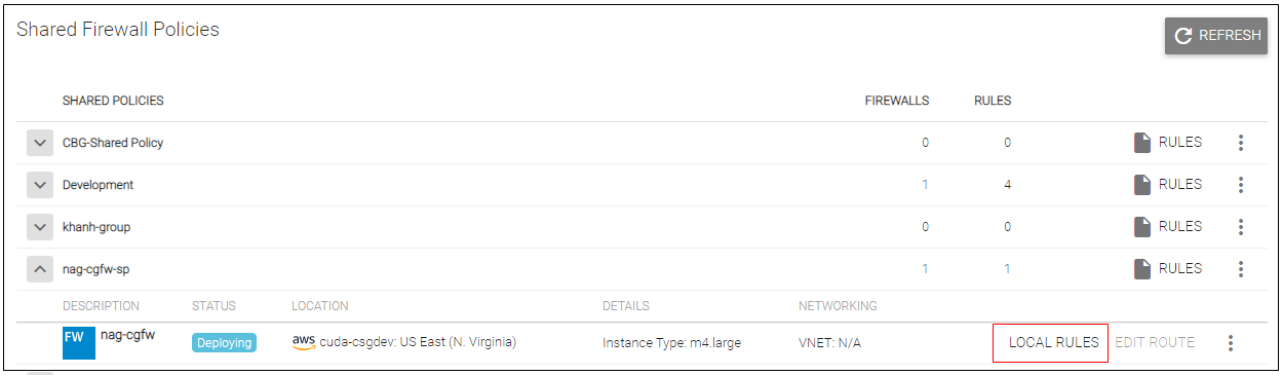
   Domain Rules – Outbound rules specific to domains you would like to connect.
   Specify the following information, then click **Add** .
   - **Name** – Specify a unique name for this new rule.
   - **Protocol** –Select the protocol to use for this rule: **TCP**, **UDP**, or **Any**.
   - **Action** – Select the type of rule, **Allow** or **Block**.
   - **Source IP Address** – Provide the Source IP Address.
   - **Host Name** – Provide the fully qualified domain name (FQDN) for this rule.

   The new rule is added and displays in the **Shared Policy Rules** window.

Local Rules

To create Local Rules for one specific firewall:

1. In the Shared Firewall Policies list, in the firewall for which you want to create a Local Rule, click **Local Rule**.



2. Select the appropriate tab to create either **Layer 4 Rules** or **NAT Rules**. Click **Add Rule**.
   Layer 4 Rules – Creates inbound and outbound layer 4 network rules.
   Specify the following information, then click **Add** .
   - **Name** – Specify a unique name for this new rule.
   - **Protocol** –Select the protocol to use for this rule: **TCP**, **UDP**, or **Any**.
   - **Action** – Select the type of rule, **Allow** or **Block**.
   - **Features** – Select either one or both: **IPS/IDS**, **Application Control**. If you choose **IDS/IPS**, you can only deploy the rule set on a Barracuda CloudGen Firewall.
   - **Source IP Address** – Provide the Source IP Address.
   - **Destination IP Address** – Provide the Destination IP Address.
   - **Port** – Provide the Port.

   NAT Rules – Outbound rules specific to domains you would like to connect.
   Specify the following information, then click **Add**.
   - **Name** – Specify a unique name for this new rule.
   - **Protocol** –Select the protocol to use for this rule: **TCP**, **UDP**, or **Any**.
   - **Source IP Address** – Provide the Source IP Address.
   - **Port** – Provide one or more ports for this rule.
   - **Translated IP Address** – The new IP address, after NAT mapping.
   - **Translated Port** – The new port, after NAT mapping.

The new rule is added and displays in the **Local Firewall Rules** window.

Detecting Existing Firewalls

The Barracuda Cloud Security Guardian automatically detects connected firewalls. Any firewall that was not added through the system is listed under **Unmanaged Firewalls** and cannot be controlled through the Barracuda Cloud Security Guardian.

Converting a Barracuda CloudGen Firewall from Unmanaged to Managed

If you have already deployed a Barracuda CloudGen Firewall and want it to be managed under Barracuda Cloud Security Guardian:

1. Enable the REST API for the Barracuda CloudGen Firewall as described in REST API for the Barracuda NextGen Firewall F-Series 7.1.
   Enabling the REST API is required and must be done before you can start to manage your firewall with Barracuda Cloud Security Guardian.
2. On the Barracuda CloudGen Firewall, open an AWS Security Group on ports `8080` and `8443`.
3. Log into your Barracuda Cloud Security Guardian account.
4. From the menu, navigate to **Policy Management > Infrastructure**.
5. On the Infrastructure Policies page, scroll down to **Unmanaged Firewalls**. Locate the Barracuda CloudGen Firewall you want to manage and, in that row, click **Link**.
6. Provide the administrative username and password for managing that firewall and click **Link**.
7. The Barracuda CloudGen firewall becomes managed and displays under a new Shared Policy group and is no longer listed under **Unmanaged Firewalls**. The new Shared Policy is named with a `<long number>_policy`. You can rename this Shared Policy.

Removing a Firewall

Removing a firewall not only removes it from management under Barracuda Cloud Security Guardian, but also removes it from your security infrastructure.

Exercise caution when removing a firewall. Removing a firewall here removes the firewall from your account entirely.

If you no longer want to manage a firewall through Barracuda Cloud Security Guardian:

1. Log into your Barracuda Cloud Security Guardian account.
2. From the menu, navigate to **Policy Management > Infrastructure**.
3. On the Infrastructure Policies page, locate the firewall you want to remove.
4. In the same row as that firewall, click the three dots ⋮ and select **Remove Firewall**.

You can watch the states change during the removal process: **Deleting** > **Finalizing** . When the process is finalized, the firewall listing is removed from the page. This process takes approximately 10 minutes.

Figures

1. CGFW1.png
2. CGFW2.png
3. cgfw3.png
4. localRules2.png
5. threeDots.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.