Get Started

https://campus.barracuda.com/doc/91985693/

Configure the Barracuda Firewall Policy Manager and set the details for administrative user groups. Settings related to authentication, security, and networking require advanced user access. The **Advanced** tab is available only for users with privileged IT Admin permissions. From here, administrators can create user groups and configure network and asset management settings. Firmware updates are performed in Barracuda Firewall Admin. To access the advanced configuration, log into the Firewall Policy Manager and click the **Advanced** tab. For a detailed description of the configuration interface, see Firewall Policy Manager Web Interface.

Configure User Groups

Add users according to your MSAD groups, and assign administrative roles so that the users can perform actions within the applications and rules creation process on the Firewall Policy Manager. System email notifications will be sent to users with appropriate roles in case of ticket status and progress changes. For a detailed description of user groups and permissions, see Administrative Roles and Permissions.

Perform the following steps for each user group:

1. In the left menu, expand **User Configuration** and select **User Groups**.
2. Click the plus icon ( ) to add a user group. The **User Group** window opens.
3. Define the following settings:
   - **Group Name** – Enter a descriptive name for the user group the configured role should be applied to.
   - **AD Group** – Select the corresponding MSAD group that contains the users in Active Directory.
   - **Role** – Select the role you wish to assign to the user group.
4. Click **Save**.

The users in the configured group are now assigned an administrative role and can perform actions they are permitted to.

Configure LDAP Settings

Configure the settings for LDAP authentication. A mapping functionality allows assigning roles in the Firewall Policy Manager to corresponding groups in Active Directory. This requires a base OU from Active Directory below which is searched. Before LDAP authentication to MSAD can work, the settings

must also be configured in Firewall Admin. For more information, see Installation and Setup.

To configure LDAP settings on the Firewall Policy Manager,

1. Go to the **Advanced** tab.
2. In the left menu, expand **User Configuration** and select **LDAP Settings**. The **LDAP Settings** window opens.
3. Define the following settings:
   - **User Filter** – Enter the format used for filtering. E.g. `objectCategory=Person`
   - **User Name Attribute** – Enter the username for authentication. E.g. `samaccountname`
   - **Group Membership Attribute** – Enter the group membership attribute. E.g. `dn`
   - **User Filter Group Part Attribute** – Enter the filtering criteria for search. E.g.: `memberOf`
   - **Login User Name Format** – Enter the format required for user login. E.g.: `%s@my.ad.int`
   - **User Base DN** – Specify the entry point in the LDAP tree for search. E.g.,: `DC=my,DC=ad,DC=int`
   - **User Email Attribute** – Enter the email attribute for authentication.
   - **Certs** – Paste your LDAP certificate. The hostname of the LDAP server must be DNS-resolvable.
4. Click **Save**.

Manage IPS Policies

Intrusion Prevention System (IPS) policies control the behavior of the IPS when an attack is detected. You can define multiple IPS policies and apply them to individual access rules as needed. By default, all access rules use the default IPS policy. All traffic is scanned according to this policy while IPS is enabled.

Create a policy that should be applied to your rules:

1. In the left menu, expand **Apps & Rules** and select **IPS Policies**.
2. Click the plus icon ( ) to add an IPS policy. The **IPS Policy** window opens.
3. In the **Group Name** field, enter the group the configured IPS policy should be applied to.
4. Click **Save**.

The policy is now listed under **IPS Policies** and can be applied to your entries.

Create Tags

Define operating environments to be selected when creating applications.

1. In the left menu, expand **Apps & Rules** and select **Tags**.
2. Click the plus icon (⊞) to add a tag. A free text field appears.
3. Enter a descriptive name for the operating environment or group the tag should be used for, and press **Enter**.

The tag is now listed under **Tags** and can be applied to your entries.

Configure Asset Management Settings

Configure the Firewall Policy Manager to use an external MSSQL database for assets used in the rules.

1. In the left menu, expand **System** and select **Asset Management**. The **Asset Management** window opens.
2. Define the following settings:
   - **Database** – Enter a descriptive name for the database that hosts your asset data.
   - **IP** – Enter the IP address of the asset management server.
   - **Port** – Enter the port the asset management server listens on.
   - **Username** – Enter the username of the user who is responsible for the asset management database.
   - **Password** – Enter the password for the user who is responsible for the asset management database.
3. Click **Save**.

The asset database is now linked to the Firewall Policy Manager, asset information is fetched from the database and can be applied to your rules.

Add Your Firewall Control Centers

When using CloudGen Firewalls that are managed by a Control Center, introduce the CC on the Firewall Policy Manager.

1. In the left menu, expand **Apps & Rules** and select **Control Centers**. The **Control Centers** window opens.
2. Click the plus icon (⊞) to add a Control Center.
3. Define the following settings:
   - **URL** – Enter the web URL with the management IP address that points to the Firewall Control Center.
   - **Port** – Select the management port the Control Center listens on.

- **Path** – Enter the path to the Control Center API location. E.g.: `/rest/cc/v1`
- **Token** – Enter the Control Center API token.

4. Click **Save**.

The Control Center is now listed in the Firewall Policy Manager configuration and rules with applications can be implemented on the managed firewalls.

Next Steps

User groups with appropriate permissions can now create applications, link applications to rules, and assign policies to firewalls in the network.

For more information, see How to Create Applications and How to Create Rules.

Figures