Installation and Setup

https://campus.barracuda.com/doc/91985184/

Installing the Firewall Policy Manager follows the same procedure as performing firmware updates and is done in Barracuda Firewall Admin. Download the Firewall Policy Manager installation file from the Barracuda download portal and install it on a dedicated CloudGen Firewall. In order to assign users that should have administrative rights to create and manage applications and rules on the Firewall Policy Manager, configure LDAP authentication.

System Requirements

- Windows Vista, Windows 7, Windows 8/8.1, or Windows 10
- 8 GB RAM
- 4 CPU cores
- 256 GB SSD storage

Browser Support

An up-to-date version of Microsoft Edge, Google Chrome, or Mozilla Firefox.

Download and Install the Firewall Policy Manager

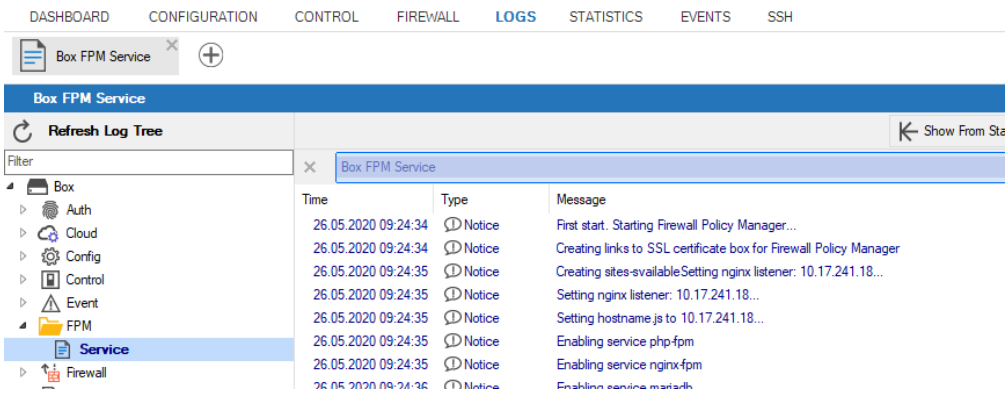
Step 1. Download the Installation File from the Barracuda Download Portal

- Go to the Barracuda download portal and download the Barracuda Policy Manager. For more information, see How to Download Applications, Updates, and Hotfixes.

Step 2. Install the Firewall Policy Manager

1. Log into the CloudGen Firewall.
2. Go to **Control > Box**.
3. In the left menu, expand the **Operating System** section and click **Install Update**.
4. Select the FPM package and upload it. For mor information, see How to Manually Install Updates via Barracuda Firewall Admin in the CloudGen Firewall documentation.
5. Reboot the CloudGen Firewall.

You can check the logs to verify that all services are running. Click the **LOGS** tab and browse to the **FPM** folder.



Step 3. Configure Network Settings

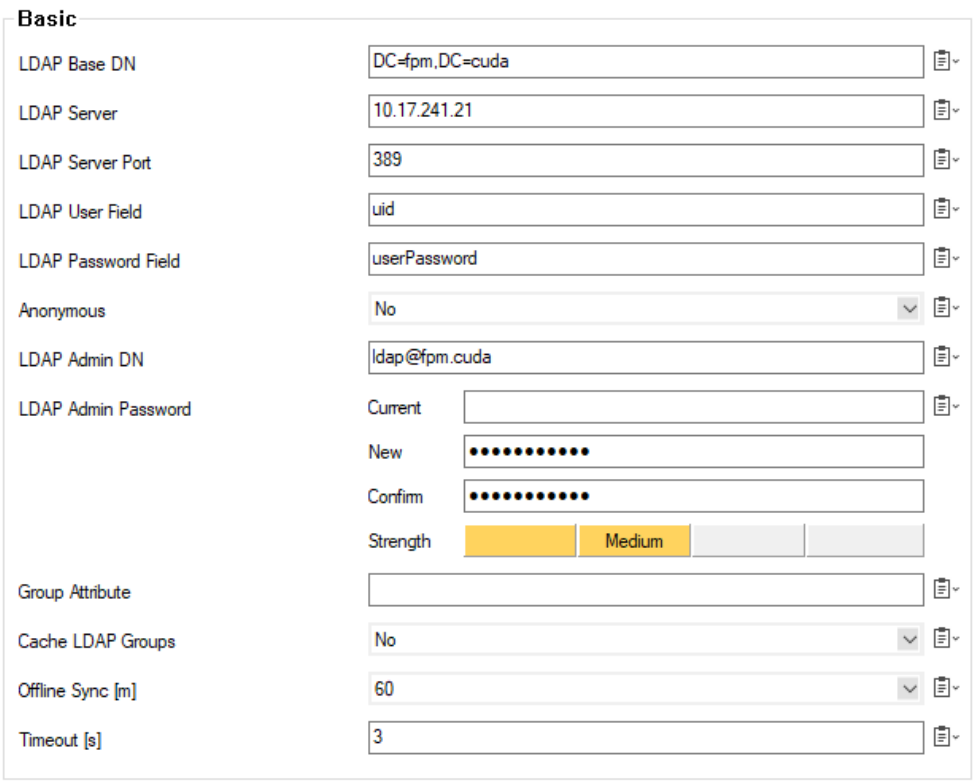
On the CloudGen Firewall, check and configure DNS and time settings and set up email notifications for the Firewall Policy Manager.

1. Go to **Box > Administrative Settings**.
2. In the left menu, select **DNS Settings**.
3. Verify that a DNS server is configured. For more information, see How to Configure DNS Settings.
4. In the left menu, select **Time Settings/NTP**.
5. Check the NTP settings and verify that **Time Server IP or Name** is configured. For more information, see How to Configure Time Server (NTP) Settings.
6. In the left menu, select **Notifications**.
7. Configure the CloudGen Firewall to send email notifications. For more information, see How to Configure System Email Notifications.

Step 4. Configure LDAP Authentication

Configure authentication settings

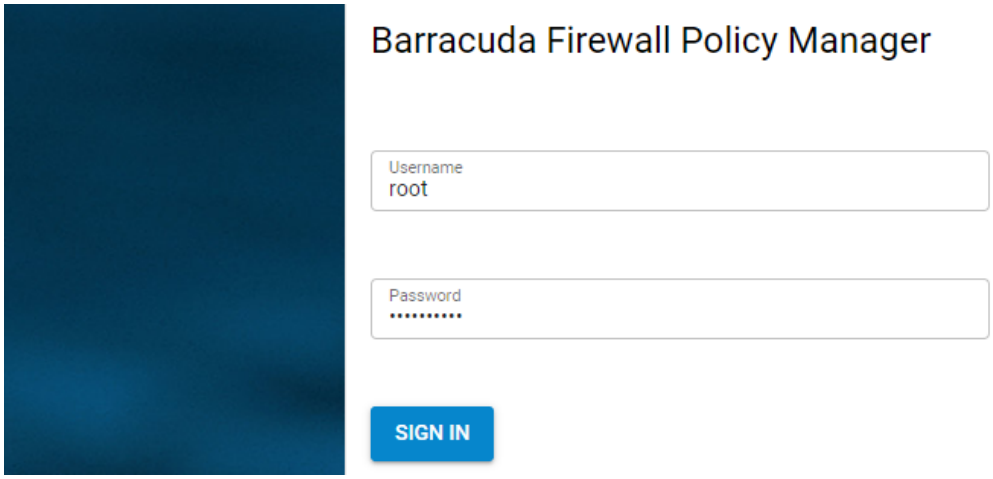
1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left navigation pane, select **LDAP Authentication**.
3. Click **Lock**.
4. Enable LDAP as external directory service.
5. In the **Basic** table, add an entry for the Base DN.
6. In the **LDAP Base DN** field, enter the Distinguished Name for the Firewall Policy Manager.
7. Enter the **LDAP Server** IP address and **LDAP Server Port** (default: port 389).
8. In **LDAP User / Password Field**, enter the name of the user identification and the password attribute in the LDAP directory. For more information on LDAP settings, see How to Configure LDAP Authentication.



9. Cick **Send Changes** and **Activate**.

Access the Firewall Policy Manager

1. Open a web browser.
2. Go to `https://<management IP address of your CloudGenFirewall>`
3. Log in with the following credentials:
   - **Username**: `root`
   - **Password**: Enter your password.
4. Click **Sign In**.



The Firewall Policy Manager web interface dashboard opens, showing the **Applications** page. For a detailed description of tabs and settings, see Firewall Policy Manager Web Interface.

Next Steps

Get started with the Firewall Policy Manager. Assign administrative user groups, link your asset management database, and configure IPS (Intrusion Prevention System). For more information, see Get Started.

Figures