Bitdefender Firewall: Overview

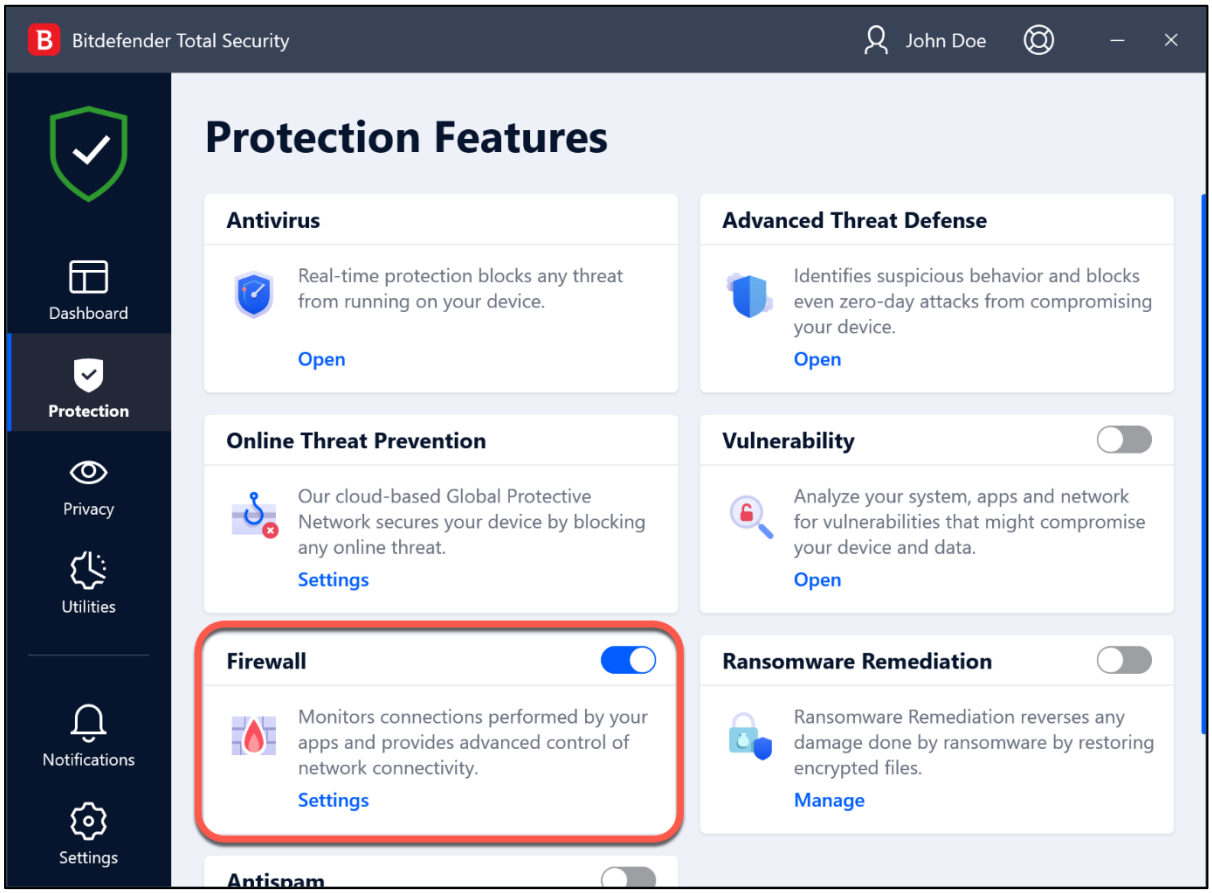
Bitdefender Firewall adds an extra layer of protection, by blocking inbound and outbound unauthorized connection attempts, both on local networks and on the Internet. It is quite similar to a guard at your gate – it keeps track of connection attempts and decides which to allow and which to block. Your personal information stays safe from hackers and data snoops. Below is basic information about the main Bitdefender firewall features. For in-depth information, please refer to the user manual.

TURNING FIREWALL ON/OFF

To enable or disable the firewall protection:

1. Open the Bitdefender interface and click **Protection** on the left side menu.

2. In the **Firewall** panel, turn on or off the corresponding switch.



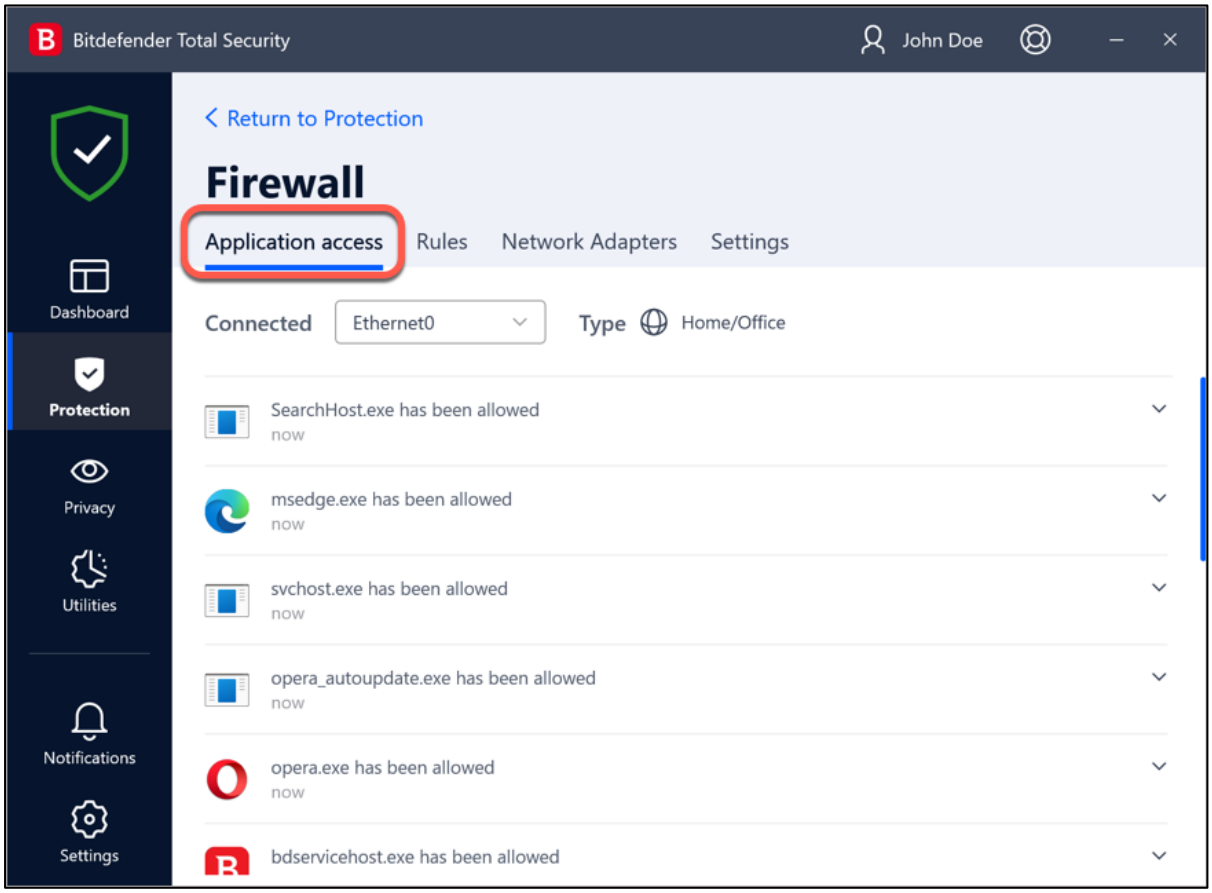
APPLICATION ACCESS

The Application Access tab shows the last 15 firewall rules added for applications that have recently accessed the Internet. To access the Application Access window:

1. Click **Protection** on the left sidebar of the Bitdefender interface.

2. In the **Firewall** panel, click **Settings**, then **Application access**.

To learn more about a certain Application access rule, click to expand it, and then choose **View application rules**. The **Rules** tab opens, where additional information is provided.



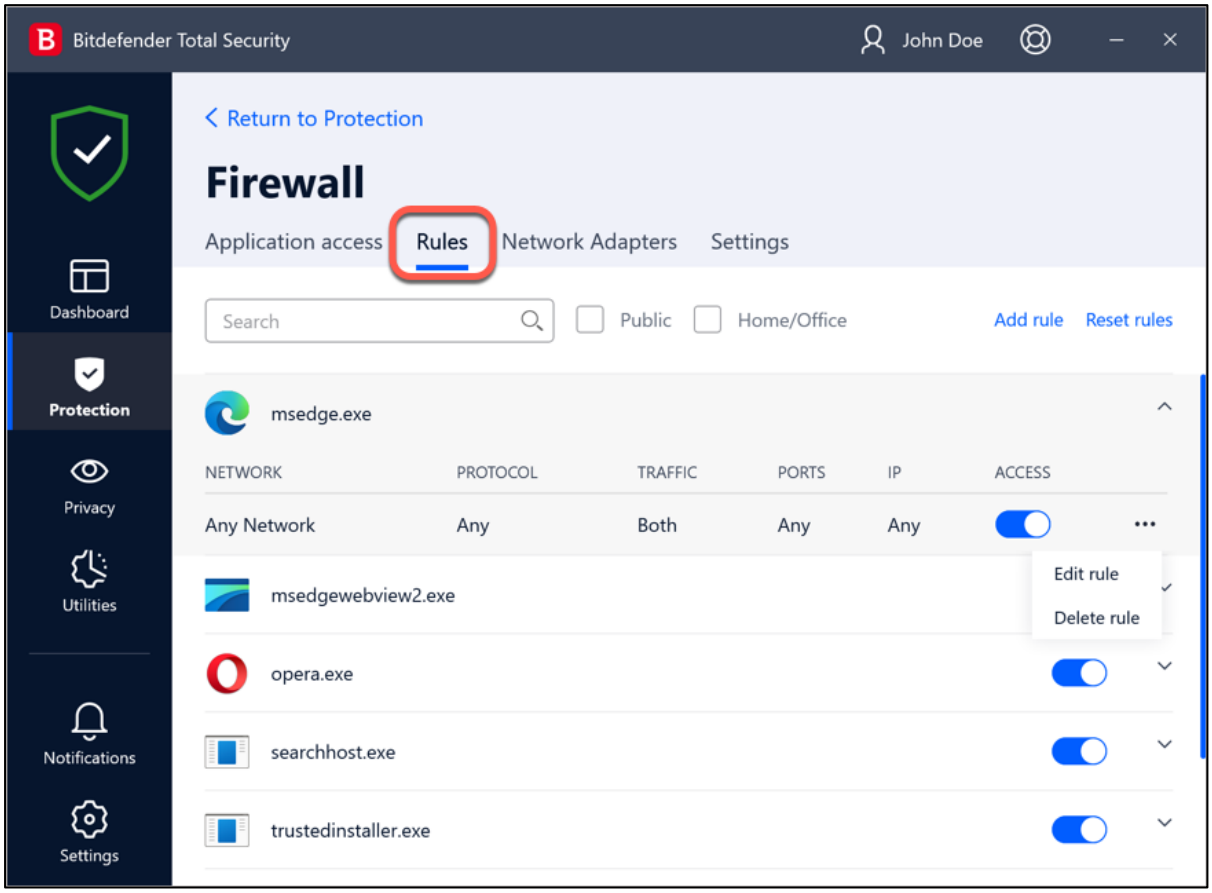
RULES

Bitdefender Firewall uses a set of rules to filter data transmitted to and from your system. It automatically creates a rule whenever an app tries to access the internet. As a safety measure, you will be notified each time a potentially malicious app is blocked from accessing the internet.

In the Rules tab, you can look up the various applications for which rules have already been created. At the same time, you can filter the rules based on the types of networks to which they apply.

You can also manually add, delete or edit app rules. To edit or delete a firewall rule click on it to expand it, then click the ellipsis ••• and select:

-
    - **Edit rule** – opens a window where you can edit the current rule.
    - **Delete rule** – you can choose to remove the current set of rules for the selected app.



For each firewall rule, the following information is displayed:

Network

That is the process and the network adapter types of the rule applies to. Rules are automatically created to filter network or Internet access through any adapter. By default, the rules apply to any network. You can manually create rules or edit existing rules to filter an application's network or Internet access through a specific adapter (for example, a wireless network adapter).

Protocol

The IP protocol the rule applies to. By default, the rules apply to any protocol.

Traffic

The rule applies in both directions, inbound and outbound.

Ports

The PORT protocol the rule applies to. By default, the rules apply to any port.

IP

The internet protocol (IP) the rule applies to. By default, the rules apply to any IP address.

Access

Whether the application is allowed or denied access to the network or internet under the specified circumstances.

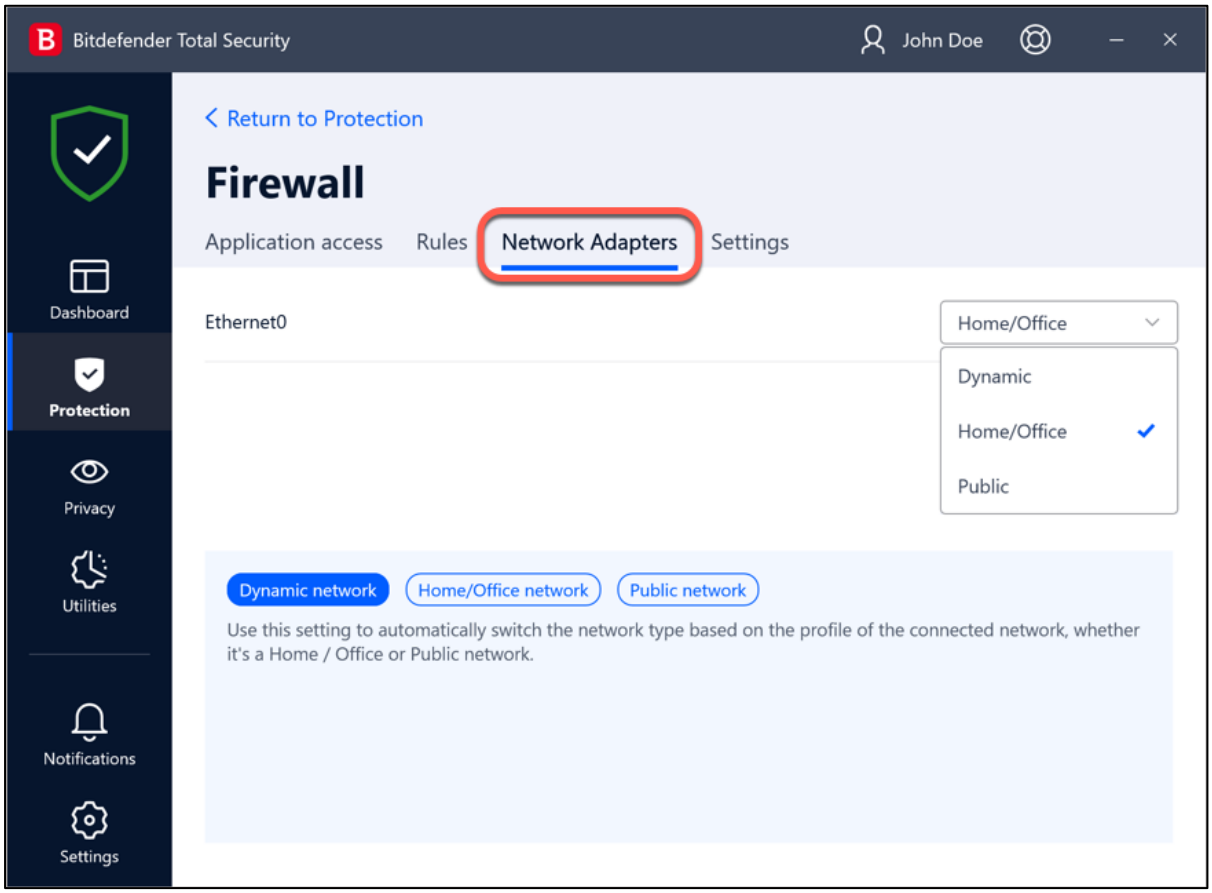
NETWORK ADAPTERS

Bitdefender automatically assigns a network type to every network connection it detects. Depending on the network type, the firewall protection is set to the appropriate level for each connection. Whether you connect to the internet using a Wi-Fi or Ethernet adapter, you can configure what settings should be applied for safe navigation. The options you can choose from, are:

Dynamic – the network type will be automatically set based on the profile of the connected network, Home/Office, or Public. When this happens, only Firewall rules for the specific network type or those defined to apply to all network types will apply.

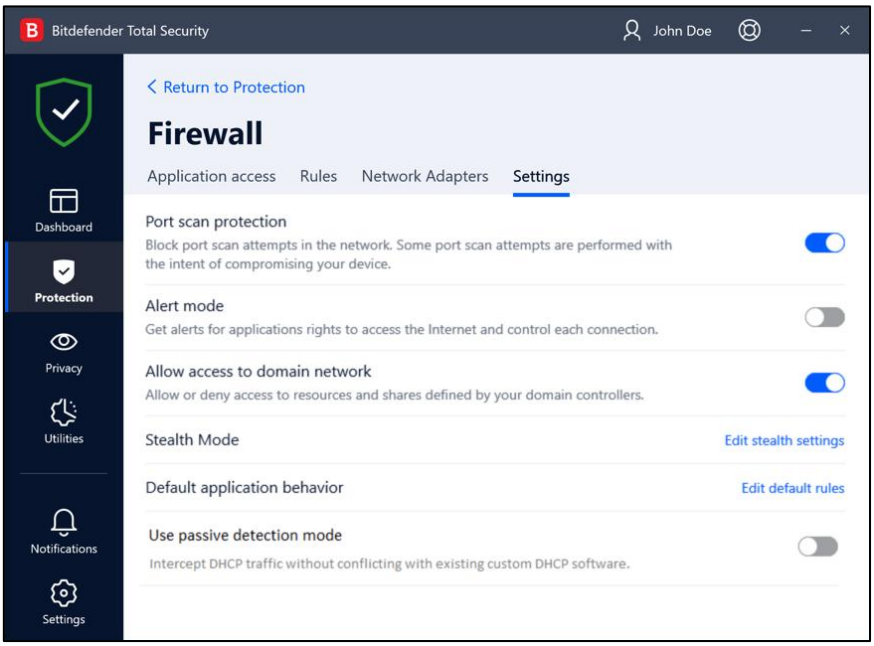
Home/Office – the network type will always be Home /Office, disregarding the profile of the connected network. When this happens, only Firewall rules for Home/Office or those defined to apply to all network types will apply.

Public – the network type will always be Public, disregarding the profile of the connected network. When this happens, only Firewall rules for Public or those defined to apply to all network types will apply.



SETTINGS

The following advanced settings can be configured here:



Port scan protection – detects and blocks attempts to find out which ports are open. Port scans are frequently used by hackers to find out which ports are open on your device. They might then break into your device if they find a less secure or vulnerable port.

Alert mode (former Paranoid Mode) – alerts are shown each time an app tries to connect to the internet. Select Allow or Block. When Alert mode is turned on, the Profiles feature is automatically switched off. Alert mode can be used simultaneously with Battery Mode.

Allow access to domain network – allow or deny access to resources and shares defined by your domain controllers. This option is visible only if the PC belongs to a domain network.

Stealth Mode – establishes whether you can be detected by other devices. Click the "Edit stealth settings" to choose when your device should or should not be visible to other computers.

Default application behavior – allows Bitdefender firewall to apply automatic settings to applications with no defined rules. Click "Edit default rules" to choose whether automatic settings should be applied or not.

Use passive detection mode – concerns Dynamic Host Configuration Protocol (DHCP) device detection. When this setting is off, the Bitdefender firewall listens for DHCP packets only on port 67 UDP. When it's on, the firewall listens and receives all packets without interfering with DHCP servers that run on the local machine.