About the application firewall

OS X includes an application firewall you can use to control connections made to your computer from other computers on your network.

OS X v10.5.1 and later include an application firewall you can use to control connections on a per-application basis (rather than a per-port basis). This makes it easier to gain the benefits of firewall protection, and helps prevent undesirable apps from taking control of network ports open for legitimate apps.

Configuring the application firewall in OS X v10.6 and later

Use these steps to enable the application firewall:

1. Choose System Preferences from the Apple menu.
2. Click Security or Security & Privacy.
3. Click the Firewall tab.
4. Unlock the pane by clicking the lock in the lower-left corner and enter the administrator username and password.
5. Click "Turn On Firewall" or "Start" to enable the firewall.
6. Click Advanced to customize the firewall configuration.

Configuring the Application Firewall in Mac OS X v10.5

Make sure you have updated to Mac OS X v10.5.1 or later. Then, use these steps to enable the application firewall:

1. Choose System Preferences from the Apple menu.
2. Click Security.
3. Click the Firewall tab.
4. Choose what mode you would like the firewall to use.

Advanced settings

Block all incoming connections

Selecting the option to "Block all incoming connections" prevents all sharing services, such as File Sharing and Screen Sharing from receiving incoming connections. The system services that are still allowed to receive incoming connections are:

- configd, which implements DHCP and other network configuration services
- mDNSResponder, which implements Bonjour
- racoon, which implements IPSec

To use sharing services, make sure "Block all incoming connections" is deselected.

Allowing specific applications

To allow a specific app to receive incoming connections, add it using Firewall Options:

1. Open System Preferences.
2. Click the Security or Security & Privacy icon.
3. Select the Firewall tab.
4. Click the lock icon in the preference pane, then enter an administrator name and password.
5. Click the Firewall Options button
6. Click the Add Application (+) button.
7. Select the app you want to allow incoming connection privileges for.
8. Click Add.
9. Click OK.

You can also remove any apps listed here that you no longer want to allow by clicking the Remove App (-) button.

Automatically allow signed software to receive incoming connections

Applications that are signed by a valid certificate authority are automatically added to the list of allowed apps, rather than prompting the user to authorize them. Apps included in OS X are signed by Apple and are allowed to receive incoming connections when this setting is enabled. For example, since iTunes is already signed by Apple, it is automatically allowed to receive incoming connections through the firewall.

If you run an unsigned app that is not listed in the firewall list, a dialog appears with options to Allow or Deny connections for the app. If you choose Allow, OS X signs the application and automatically adds it to the firewall list. If you choose Deny, OS X adds it to the list but denies incoming connections intended for this app.

If you want to deny a digitally signed application, you should first add it to the list and then explicitly deny it.

Some apps check their own integrity when they are opened without using code signing. If the firewall recognizes such an app it doesn't sign it. Instead, it the "Allow or Deny" dialog appears every time the app is opened. This can be avoided by upgrading to a version of the app that is signed by its developer.

Enable stealth mode

Enabling stealth mode prevents the computer from responding to probing requests. The computer still answers incoming requests for authorized apps. Unexpected requests, such as ICMP (ping) are ignored.

Firewall limitations

The application firewall is designed to work with Internet protocols most commonly used by applications – TCP and UDP. Firewall settings do not affect AppleTalk connections. The firewall may be set to block incoming ICMP "pings" by enabling Stealth Mode in Advanced Settings. Earlier ipfw technology is still accessible from the command line (in Terminal) and the application firewall does not overrule any rules set using ipfw. If ipfw blocks an incoming packet, the application firewall does not process it.

Published Date: April 03, 2020