GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

P

Personal Firewall: Inbound and Outbound Rules Explained

A personal firewall filters network traffic on one device. Learn the difference between inbound and outbound rules, profiles, safe defaults, and limitations.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

CONTENTS

In this guide

01 What a personal firewall does
02 Inbound versus outbound rules
03 Public, private, and domain profiles
04 Safe setup checklist
05 When an application stops working
06 What a personal firewall cannot do
07 Source

Quick answer: A personal firewall is software on an individual computer that allows or blocks network traffic according to rules. Keep it enabled, use the correct network profile, deny unsolicited inbound connections by default, and create narrow exceptions only for

applications and services you trust. It complements a router and antivirus; it does not replace either.

01 What a personal firewall does

A personal firewall, also called a host-based firewall, sees traffic entering and leaving one endpoint. It can evaluate protocol, local and remote address, port, application, user, service, and the network profile in use. This lets a laptop apply stricter rules on airport Wi-Fi than on a managed company network.

A router or network firewall protects a boundary shared by multiple devices. A personal firewall remains with the endpoint, including when it moves outside that boundary, and can limit connections from another compromised device on the same internal network. Using both provides layered protection.

02 Inbound versus outbound rules

Inbound rules control connections initiated toward the device. A safe consumer default is to block unsolicited inbound traffic and allow responses to connections the device initiated. File sharing, remote desktop, development servers, and games may need exceptions, but those exceptions should be limited to the required profile, program, port, and trusted source addresses.

Outbound rules control connections initiated by local applications. They can stop an unknown program from reaching the network, but strict outbound allow-listing requires maintenance. Many legitimate apps update, change paths, use content-delivery networks, or need dynamic destinations. Randomly approving every prompt defeats the control; organizations should base outbound rules on an inventory and review logs.

03 Public, private, and domain profiles

- **Public:** use the most restrictive profile for hotels, cafés, airports, and other untrusted networks. Disable discovery and sharing unless essential.

- **Private:** appropriate only for a home or other network you control. It may permit selected discovery or sharing.
- **Domain or managed:** controlled by organizational policy after the device authenticates to the company environment.

Do not mark an unfamiliar network as private just to make an app work. Correct the rule or troubleshoot the service instead.

04 Safe setup checklist

1. Enable the operating system firewall on every profile and confirm another security suite has not silently disabled it.
2. Remove obsolete exceptions. Prefer application or service rules over opening a port to every program.
3. Limit scope to the smallest necessary addresses, ports, direction, and profile. Avoid “any/any” rules.
4. Turn on logging for blocked connections and, where useful, allowed connections. Protect and rotate the logs.
5. Test from another device. A listening port alone does not prove it is reachable through the firewall.

05 When an application stops working

Confirm which executable owns the connection, its direction and port, the active profile, and whether the remote address changes. Check the firewall log before disabling protection. Create a temporary narrow rule, test it, and remove it if it does not solve the problem. Never leave the firewall off as a permanent workaround.

06 What a personal firewall cannot do

A firewall cannot reliably identify every malicious action inside allowed HTTPS traffic, undo stolen credentials, scan a file like antivirus, or protect a device that is no longer patched. Malware running with administrator control may alter local rules. Use endpoint protection, software updates, least privilege, MFA, backups, and network monitoring alongside it.

07 Source

The host-firewall definition and layered deployment guidance align with NIST Special Publication 800-41 Revision 1.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com