ESET Tech Center

ESET Endpoint Security Personal firewall behavior and user interaction (5.x)

Ondersteuning | ESET Nederland - 2024-08-28 - Reacties (0) - 5.x

https://support.eset.com/kb3559

Issue

Change the filtering mode of the ESET Personal firewall

Learn about the different filtering modes available for the ESET Personal firewall

Details

Solution

Explanation of filtering modes

Change the ESET Personal firewall filtering mode from ESET Remote Administrator

Change the ESET Personal firewall filtering mode on individual client workstations

Explanation of filtering modes

Automatic mode — In Automatic mode, network communication is automatically controlled by settings defined by the user. In ESET Endpoint Security version 6 and earlier, it was possible to select **Automatic mode with exceptions**. Later versions of ESET Endpoint Security always incorporate any user-defined exceptions that have been created automatically when operating in Automatic

mode.

After connecting to a network, ESET Endpoint Security will prompt you to define whether that network is included in a trusted zone. Communication in a trusted zone is allowed in both directions. Communication in a restricted zone is allowed only for applications that establish outgoing connections. Once an application initiates an outgoing connection, it is allowed to create an incoming connection in Automatic mode. Automatic mode requires no user interaction (except when connecting to a new network) and does not use any predefined rules out-of-the-box.

Automatic mode with exceptions (user-defined rules) — The same behavior as Automatic mode, but the administrator or user can create custom rules.

Interactive mode — In Interactive mode, network communication is handled according to predefined rules. If there is no rule available for a connection, the user is prompted to allow or deny the connection. After some time, the user will have created a group of rules fitting his or her needs. Use caution when choosing this mode in a corporate environment because users who do not pay attention to each prompt can accidentally create a rule that might expose them to risk or hinder their ability to communicate over the network.

Policy-based mode — In Policy-based mode, network communication is handled according to rules defined by the administrator. If there is no rule available, the connection is automatically blocked and the user sees no warning message. We recommend that you only select Policy-based mode if you are an administrator who intends to control network communication and you

are sure you know which applications should be allowed or denied.

Learning mode — Learning mode should only be used if you are an experienced user in a controlled environment because it does not require user approval to create permanent rules and can expose your computer to increased risk.

Learning mode allows all activity and automatically creates and saves rules based on user behavior; it offers a less user-intensive initial configuration of the Personal firewall. No user interaction is required. Learning mode is not secure, and should only be used until all rules for required communications have been created. The Personal firewall should then be set to Automatic mode with exceptions or Policy mode.

Change the ESET Personal firewall filtering mode from ESET Remote Administrator

> If you do not use ESET Remote Administrator to manage your network
>
> Perform these steps on individual client workstations.

1. Open the ESET Remote Administrator Console by clicking **Start → All programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**.

2. Click **Tools → Policy Manager**.

3. Select your server policy and click **Edit Policy**.

Figure 1-1

Click the image to view larger in new window

4. Expand **Windows desktop v5 → Personal firewall → Settings** and click **Filtering mode: [value]**.

5. Select your desired filtering mode from the **Value** drop-down menu.

Figure 1-2

Click the image to view larger in new window

6. Click **Console** and the click **Yes** to save your changes.

Figure 1-3

Click the image to view larger in new window

Change the ESET Personal firewall filtering mode on individual client workstations

1. Open ESET Endpoint Security. How do I open my ESET product?
2. Click **Setup → Network**.

Figure 2-1

Click the image to view larger in new window

3. Click **Advanced Personal firewall setup**.

Figure 2-2

Click the image to view larger in new window

4. Expand **Network → Personal firewall**. Select your desired filtering mode from the **Filtering mode** drop-down menu and click **OK** to save your changes.

Figure 2-3

Click the image to view larger in new window

Tags

EES

ERA 5.x

Policy