

ESET

Personal Firewall

User Guide



we protect your digital worlds

Contents

1. Introduction	3
2. ESET Personal firewall concepts	4
2.1 Filtering modes in ESET Personal firewall	4
2.2 Zones.....	7
2.3 Strict rules & security levels	8
2.4 Rule configuration strategy for large networks	9
3. Creating rules and zones in the ESET graphical interface.....	10
3.1 Detection of modified applications	13
3.2 Logging network activity	14
3.3 XML Configuration files & ESET Configuration Editor	16
4. Summary.....	17

ESET Personal Firewall

Copyright © 2008 by ESET, spol. s r.o.

ESET Personal Firewall was developed by ESET, spol. s r.o.
For more information visit www.eset.com.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o., reserves the right to change any of the described application software without prior notice.

Customer Care Worldwide: www.eset.eu/support
Customer Care North America: www.eset.com/support

REV.20080303-001

1. Introduction

The ESET Smart Security architecture integrates Antivirus, Antispyware, Antispam, and the Personal firewall. Each of these components can be configured and managed through the ESET Remote Administrator (ERA). This manual describes how to deploy the Personal firewall in a network environment, as well as instructions on remote management of the Personal firewall using ERA. Why install a Personal firewall on client computers, when there is a central firewall on the company's server? There are several reasons:

- A Personal firewall can eliminate attacks from within the local network (e.g., an infected guest notebook connecting to the corporate network).
- A Personal firewall allows the administrator to effectively limit communication in order to decrease network traffic, which may be an issue for remote locations or WAN connections (e.g., a rule could be created to block all instant messaging applications and only allow the use of local SMTP servers).
- A Personal firewall can prevent malicious code from spreading further, by eliminating its ability to reach other computers and cause further damage (e.g., when a trojan horse uses its own SMTP engine to send spam messages and malicious code).

2. ESET Personal firewall concepts

2.1 Filtering modes in ESET Personal firewall

ESET Personal firewall supports three filtering modes:

- **Automatic**

This mode automatically allows all standard outgoing connections and blocks all non-initiated incoming connections. Incoming connections initiated on the local computer are allowed. The Personal firewall uses a predefined set of rules provided by ESET which are suitable for most users, since there is no need for any user intervention – aside from setting up a Trusted zone – no special networking knowledge is required.

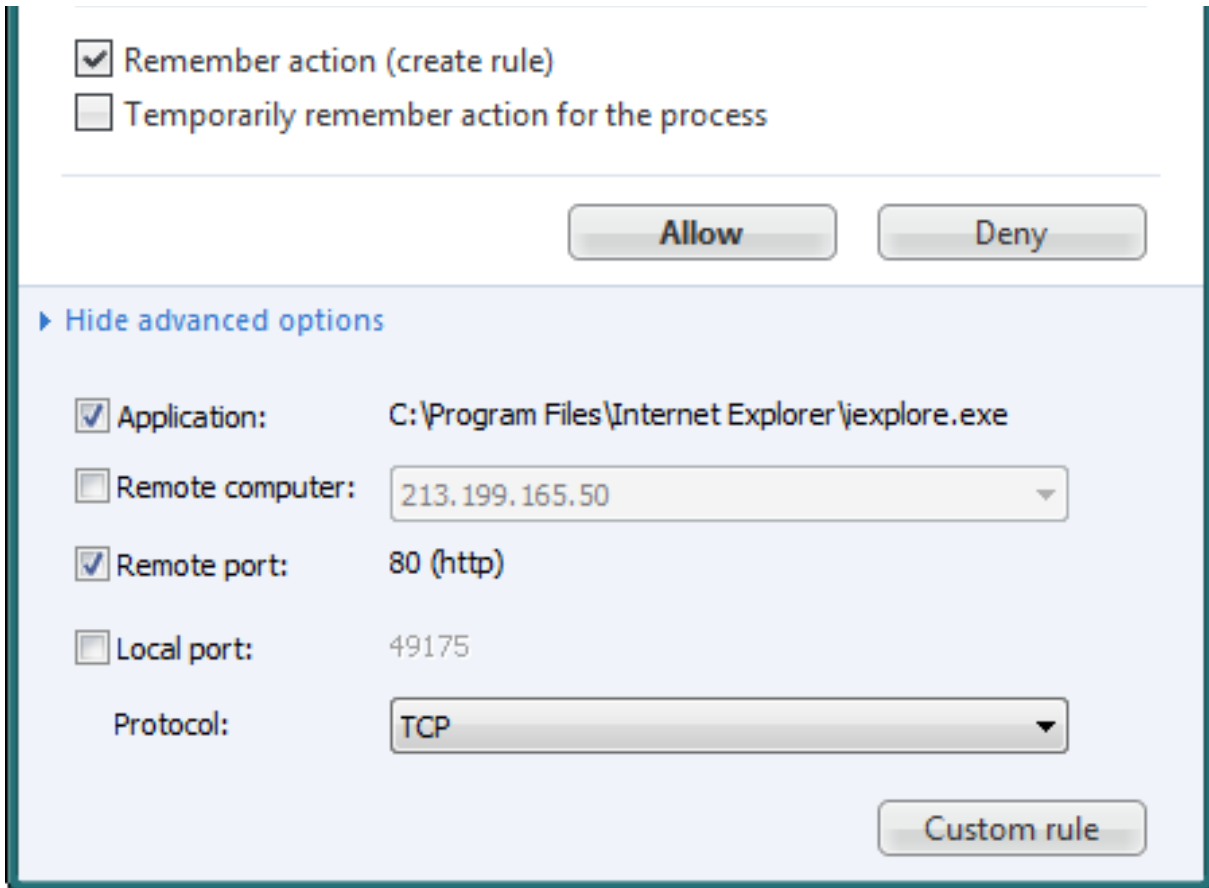
- **Interactive**

This mode is based on user-defined rules, as well as a basic set of predefined rules. If a rule already exists to allow or deny a specific type of communication, that rule is automatically applied. For communications where no rules have been defined, the user is prompted to allow or deny the communication. If neither check box is selected in the dialog window, then the permission (or denial) applies only to the current instance and no permanent rule is created.



If you select the **Temporarily remember action** check box for this process, the action you choose is bound to the PID (process ID) of the process. Unless the PID changes, no additional dialog windows regarding that communication will be displayed. Temporary rules are automatically deleted after the computer is restarted.

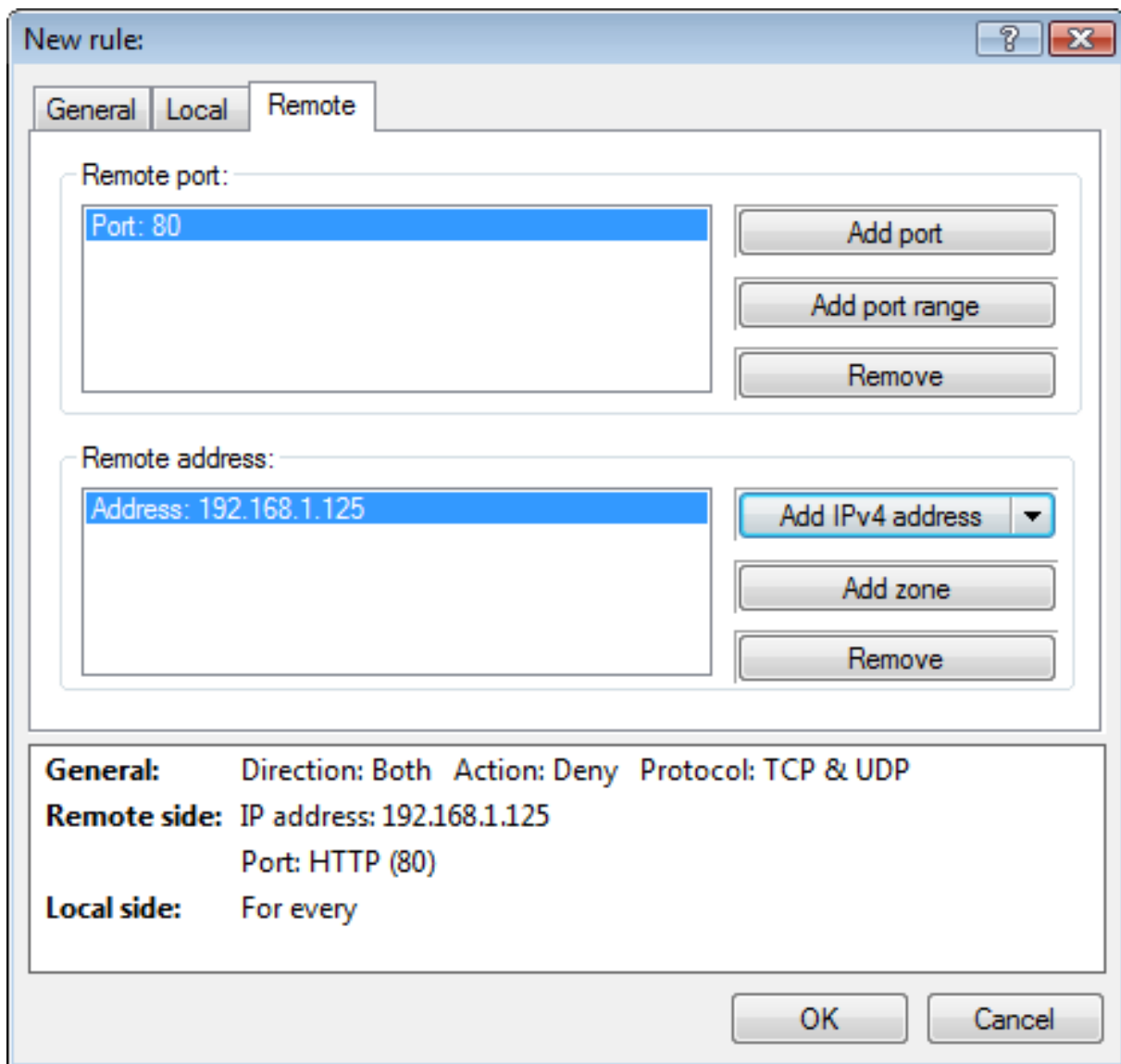
Select the **Remember action** option and select **Allow** or **Deny** to create a permanent rule for the communication. If a similar communication occurs in the future, it is automatically allowed or blocked. However, such rules are very general, since they would always allow all incoming and outgoing communications (for all target ports, all IP addresses...) for the given process. To specify more detailed parameters for a specified rule, click **Show advanced options**. The figure below shows an example of limiting the HTTP communication (port 80) established by the Internet Explorer web browser.



In addition to port 80 (HTTP), you may wish to allow communication on port 443 (HTTPS). There are three ways to accomplish this:

- o Wait until the web browser establishes communication on port 443 (e.g., when you log in to your online banking account). You will be prompted to create an *additional* rule for the same application (Internet Explorer and the process iexplore.exe).
- o Click **Custom rule** to open a dialog window and specify detailed settings for the rule. You can add specific ports, IP addresses, IP address ranges, etc. In this case, all communication for the given application would be specified by only *one* rule.¹

¹ If you want an application to behave differently within and outside the Trusted zone, or if you have different rules exclusively for incoming or outgoing communication (for the same application) more than one rule would be required.



o Avoid the dialog windows which are displayed in Interactive mode by specifying rules manually in the Personal firewall Zone and rule editor. Manual rule definition is also implemented when using the Policy-based filtering mode, explained below.

- **Policy-based**

In this filtering mode only predefined rules are used. For communications where no rules have been defined, the connection is denied and no dialog window is displayed. This is the main difference between Interactive and Policy-based mode. Policy-based mode is well-suited to large corporate networks where communication is strictly managed and controlled by the administrator.

In summary, the following statement is true for all filtering modes:

Any communication for which there is no match among existing rules, is automatically blocked (Automatic and Policy-based mode), or a dialog window requiring user intervention is displayed (Interactive mode).

2.2 Zones

In addition to rules, zones also play an important role. A zone can be defined by any of the following:

- individual IP address (for example 192.168.1.1)
- IP Address range (from 192.168.1.1 to 192.168.1.5)
- subnet (192.168.1.0 / mask 255.255.255.0, which means addresses from 192.168.1.1 to 192.168.1.255)

A zone can contain a single IP address or several IP addresses defined by a range or subnet. You can also specify groups of IP addresses, which can be useful when creating rules. Some zones are predefined and can't be modified or removed. These zones are listed below:

- **Trusted zone**

The Trusted zone consists of IP addresses, address ranges or subnets which are recognized by the Personal firewall as safe. Adding IP addresses or ranges to this category will change the behavior of ESET Smart Security when accessing shared folders and printers. If any computer is assigned a different IP address not belonging to the Trusted zone, the Personal firewall will treat that network as not trusted.

- **Networks marked as Not trusted**

The opposite of the Trusted zone. It should list all IP addresses, address ranges and subnets that are automatically treated as not trusted. In such a network, shared folders and printers are by default disabled, and the computer will not be visible to other computers in the network.

- **DNS servers**

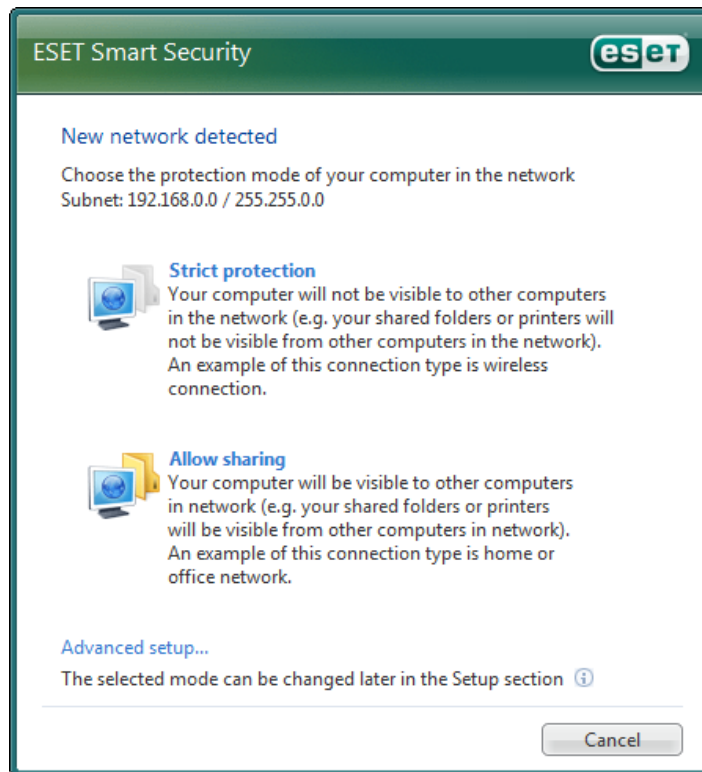
Specifies DNS servers which client is allowed to use.

- **Local addresses**

Specifies IP addresses by which the client is represented (usually contains the IP address 127.0.0.1 and IP addresses assigned to all network adapters).

Zones can also be used for specifying strict rules in the Personal firewall.

The behavior of the Personal firewall in a new network is determined by the option **Do not display dialog with Trusted zone settings when changes in the network adapter settings are detected** (e.g., change of IP address), located in **Advanced setup... > Personal firewall > Rules and zones**. If this option is enabled and the computer receives communication by an IP address not specified by the Trusted zone, then this subnet is automatically treated as not trusted (see **Strict Protection**, below).



NOTE: The **New network detected** window is not displayed if the computer's IP address belongs to a subnet which doesn't contain any other IP addresses (mask 255.255.255.255), or is a public IP address. In both cases, the subnet is treated as not trusted.

Zones can be used to create rules on a per network basis. The examples below show two separate networking scenarios and a solution for each:

Task 1:

FTP communication should be enabled in the local network, and disabled outside the LAN, except for the public IP addresses 217.67.22.98 and 72.32.7.91.

Solution 1:

Create a new zone, add the IP addresses 217.67.22.98 and 72.32.7.91 and name it "Internet FTP servers". Create a new rule allowing outgoing FTP communication. On the **Remote** tab, add the zones "Trusted zone" and "Internet FTP servers".

Task 2:

Client computers need to use DNS services within the local network. These services mustn't be accessible from outside the network (i.e., from the Internet), because the server is also an Internet gateway for the network.

Solution 2:

Create a new rule named "DNS for client computers", using the following parameters:

General tab - Direction: **IN**, Action: **ALLOW**, Protocol: **UDP**.

Local tab - Local port: 53 (**DNS**).

Remote tab - Zone: **Trusted zone**.

2.3 Strict rules & security levels

The administrator can select one of the following scenarios for deployment of the ESET Smart Security Personal

firewall:

- Leave **Automatic filtering mode** enabled on the Personal firewall and redefine the Trusted zone, if necessary. With this configuration, users will not be prompted to select a protection mode if they connect to a new network (e.g., with mobile devices such as notebooks). Keep in mind that outgoing communication will not be completely filtered.
- Select the **Interactive filtering mode** in the Personal firewall. This mode is not suitable for inexperienced users, since any new communication not specified by a rule will prompt to create one. This may cause problems and is not recommended.
- Switch to the **Policy-based filtering mode** in the Personal firewall and create more “lenient” rules. For example, all SMTP, HTTP and POP3 communication would be allowed, regardless of the application establishing them. Such rules should be set up by an experienced network administrator.
- Select the **Policy-based filtering mode** in the Personal firewall with additional rules which dictate that certain networking services can only be used by specific applications or processes. For example, communication for the process firefox.exe will be allowed only on remote ports 80 (HTTP) and 443 (HTTPS); Outlook Express only on ports 25, 110, 143 and limited to the IP addresses where the company’s email servers are located, etc.

This last scenario is the most complex and may require fine-tuning of some rules, but it also offers the highest level of security. For example: Malicious code which is not recognized by the resident antivirus protection attacks a computer. The code creates a local SMTP server and sends spam messages on behalf of a remote web server from a predefined public IP address. This type of infiltration will be automatically blocked in the last scenario, because SMTP communication is enabled only for Outlook Express and HTTP traffic only for Mozilla Firefox.

2.4 Rule configuration strategy in large networks

If you wish to set the most strict level of network access for client computers, use **Policy-based filtering mode**, because it allows no user intervention.² The successful deployment of Policy-based mode requires thorough preparation, as blocking of legitimate applications must be avoided. There are several methods for deploying Policy-based mode:

- Define rules “from scratch” and directly install ESET Smart Security with Policy-based mode turned on. The risk is that you may forget to specify rules for some applications and their communication will be automatically blocked.
- First install ESET Smart Security, switch to Interactive filtering mode, and define rules “on-the-fly” as individual communications occur during regular operation of the system. If a new communication is detected (no rule is defined), a dialog window requiring user intervention is displayed. If it is a common and legitimate communication, you may want to define a rule immediately. Typically, the rule configuration process takes several days to complete, as rules for all applications must be created through regular interaction with the network. This is the recommended method.

TIP: After using Interactive mode for several days, switch to Policy-based filtering mode and export the ESET Smart Security settings (including all rules) to an .xml file. The settings can then be exported using ESET Remote Administrator, or ESET Smart Security itself (**Setup > Import and export settings...**). The .xml configuration can then be used for remote configuration of the program to other computers or it can be imported locally using the same feature in ESET Smart Security (**Setup -> Import and export settings...**).

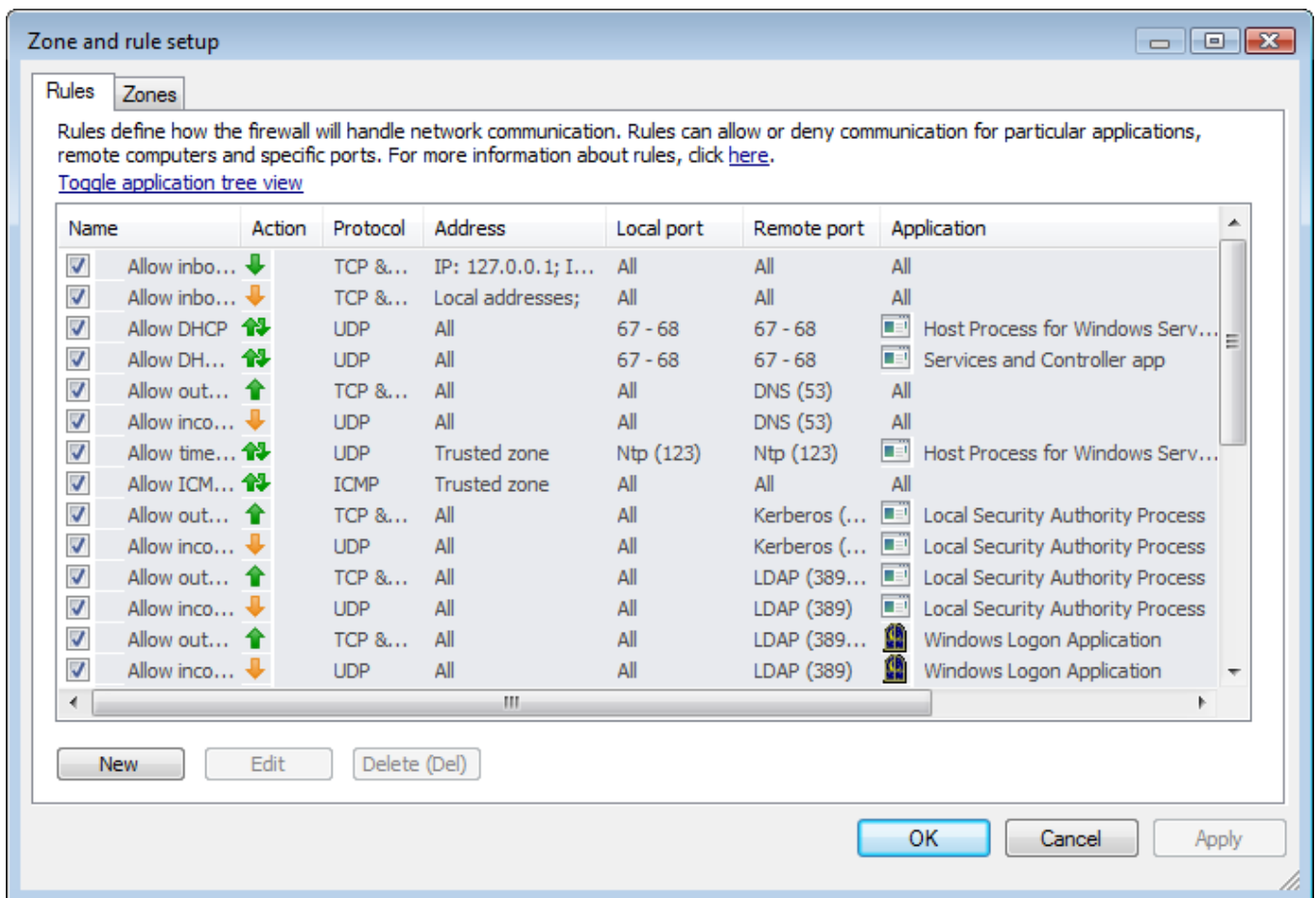
² Please note that in order to prevent users from altering Personal firewall rules, you must set a password to protect the program parameters of the ESET Smart Security client.

3. Creating rules and zones in the ESET graphical interface

Rules and zones are configured using two methods:

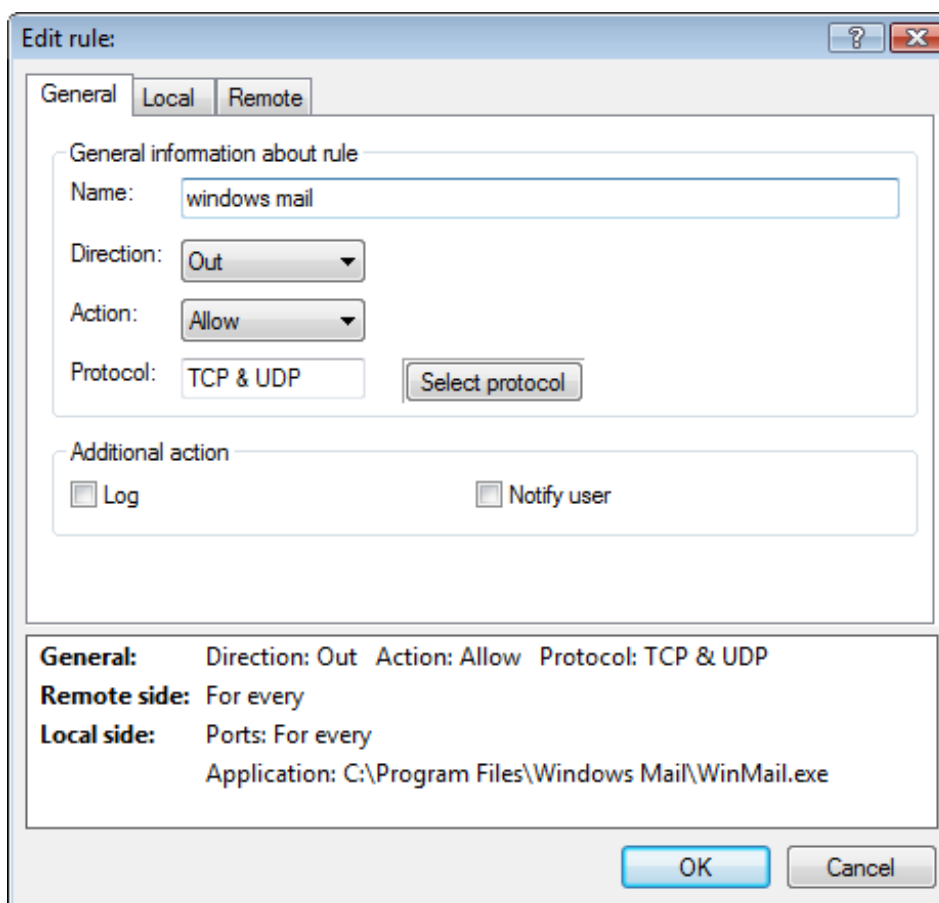
- In the Advanced Setup window of ESET Smart Security (launched by pressing the F5 key) or by navigating to **Setup > Personal firewall > Advanced Personal firewall setup...** from the main program window.
- Using the ESET Configuration Editor tool which is part of ESET Remote Administrator. The Configuration Editor can be used to open existing rules from any client computer, to open an exported .xml configuration file, or to create new program settings based on an existing configuration.

In both cases, the **Zone and rule setup** dialog windows are similar to each other.



Items with grey background mark rules defined by ESET. In certain cases, they can be partially modified using the options in the section IDS and advanced options (you can, for example, enable or disable file and printer sharing in the Trusted zone). The other rules are user defined rules. Click Toggle detailed view of all rules to toggle rule display modes. If item/rule is checked, it is active. Uncheck rules are not applied.

Double click on any item (or mark it and select the button Edit) to obtain dialog showing its detailed settings. The rule below allows communication for the email client Windows Mail.



Item	Meaning/defines
Name	name of rule
Direction	direction of communication (In, Out, Both)
Action	action to be executed (deny, allow, ask)
Protocol	protocol
Log	select this option to log the activity connected with the rule (see the chapter on logging)
Notify user	displays a message when the rule is applied
Local port	source communication port (or group of ports)
Application	the name of the application/process to which the rule applies
Remote port	target communication port (or group of ports)
Remote address	target IP address (or IP address range, or subnet)

NOTE: The rule order is not important. Only rules related to a given communication are applied to it. If no such rule exists, communication is blocked. More specific rules have priority over less specific (compare “deny communication for FTP client” and “allow FTP communication”).

The following table shows a list of typical rules. Most of these can be applied if Policy-based filtering mode is activated:

Requirement	Direction	Protocol	Local port	Application	Remote port	Remote address	Note
Enable updates for client computers with ESS	Out	TCP		ekrn.exe	80, 2221		port 80 for Internet updates, port 2221 if updating from local update server (e.g., from ERA)
Enable communication of ESS with ERA Server (client-side rule)	Out	TCP		ekrn.exe	2222, 2224		port 2224 can be used for remote installation / uninstallation.
Enable communication of ERA Console with ERA Server	Out	TCP		console.exe	2223		console side rule, if ESS is present on the same PC.
Send and receive email	Out	TCP		Process of your email client	25 (SMTP), 110 (POP3), 143 (IMAP)	IP addresses of your email servers	remote address can be filled in if you want very strict protection
Web browsing	Out	TCP		Web browser process	80 (HTTP), 443 (HTTPS), or proxy server port		
FTP client - server	Out	TCP		FTP client	21 (FTP), 1024 to 65535		passive FTP mode (recommended)
FTP client - server (active)	Out	TCP		FTP client	21 (FTP)		
Alternative to the previous rule	In	TCP & UDP		FTP client	20 (FTP-data)	IP address of FTP server	the IP address of the FTP server must be specified!
Remote desktop access to other PC	Out	TCP		mstsc.exe	3389		browse the process
Microsoft Live Messenger	Out	TCP		msnmsgr.exe	1863		browse the process
Local Apache Web Server – visible from the Internet	In	TCP	80	apache.exe			in Remote address you can specify IP addresses from which the web should be accessible (or specify them in Trusted zone)

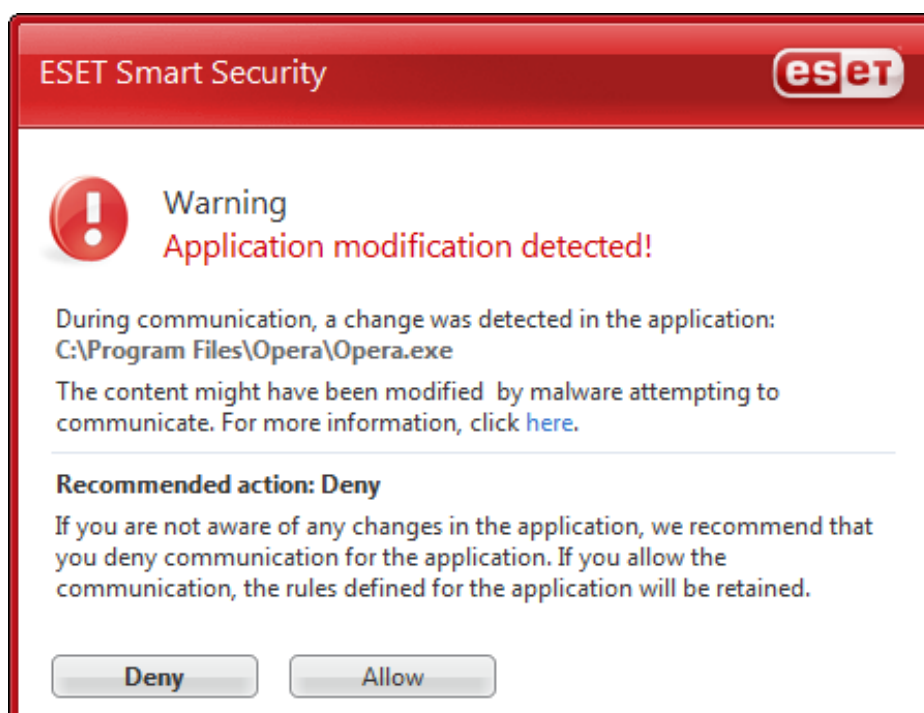
As the above list implies, you must create specific rules for handling communication within ESET Smart Security itself (updates, connection to ESET Remote Administrator Server, etc.). For security purposes, these rules are not predefined by ESET.

Please pay special attention to the svchost.exe process, as the rule configuration for this process depends on the local configuration. The RPC and DHCP communications are specified by a predefined rule (incoming RPC is enabled in Trusted zone), so you should focus primarily on the outgoing communication of svchost.exe. An ideal rule for the svchost.exe process would look like this:

Requirement	Direction	Protocol	Local port	Application	Remote port	Remote address
svchost.exe ven	Out	TCP		svchost.exe	443	update.microsoft.com, download.microsoftupdates.com, windowsupdate.microsoft.com

3.1 Detection of modified applications

The **Application modification detection** option can be found in the Advanced Setup window under **Personal firewall**. When enabled, ESET Smart Security initiates a cyclic redundancy check (CRC) for each monitored process. If the process is changed, the user is notified and prompted to allow or deny communication (see the dialog below). Select **Deny** to deactivate the corresponding rule and to deny the current communication. The behavior of this feature can be adjusted by the **Allow modification of signed (trusted) applications** option. This option checks the certificates of digitally-signed applications, which are typically found on Microsoft applications and operating system components.

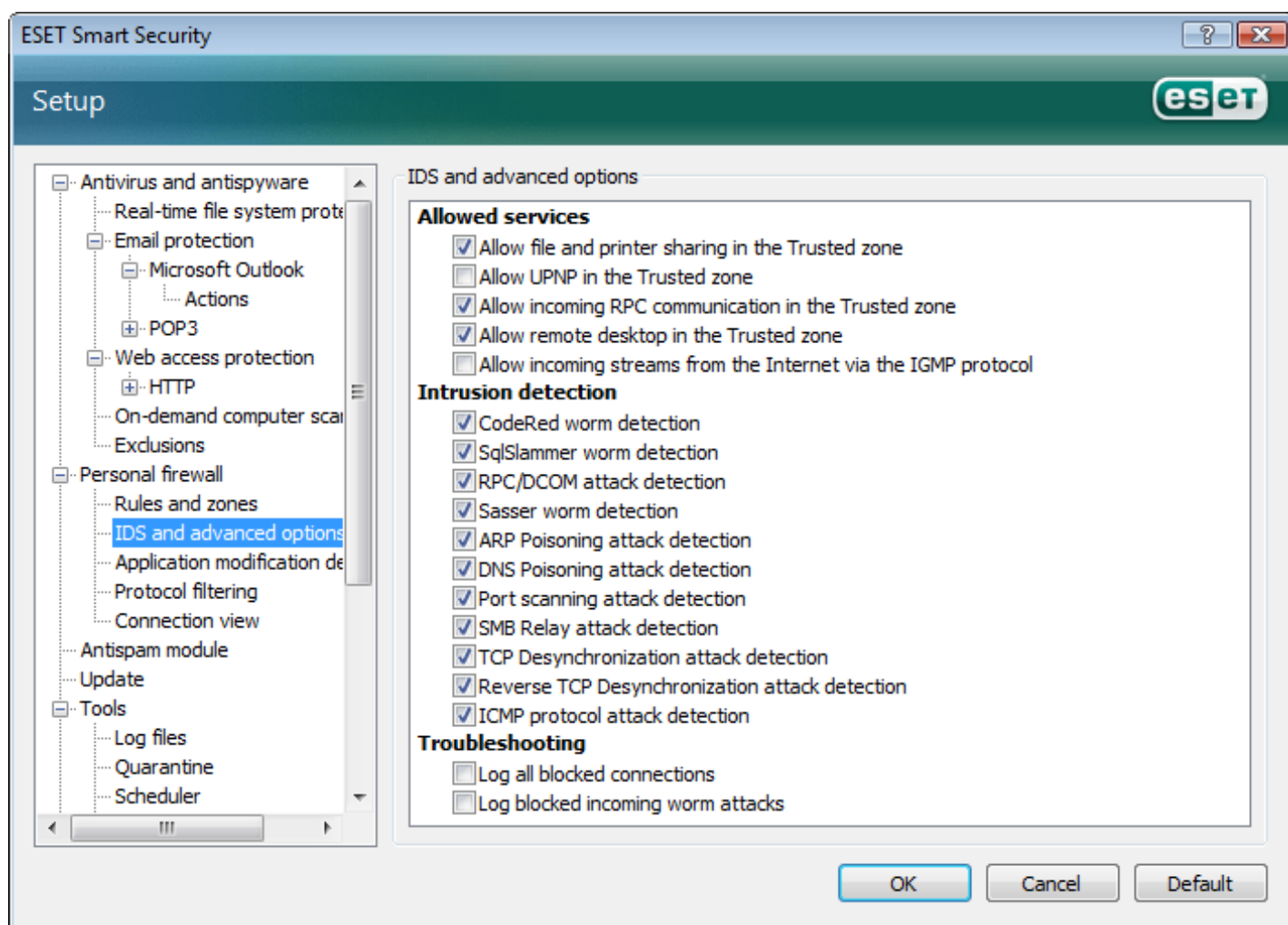


Application modification detection helps guard against malicious code which presents itself as a legitimate process. Consider a malicious program which replaces the *Outlook.exe* process with its own code for the purpose of sending unsolicited email via SMTP. Without application modification detection, the malicious code would not be stopped, since a rule exists which allows the legitimate process *Outlook.exe* to send and receive email (SMTP).

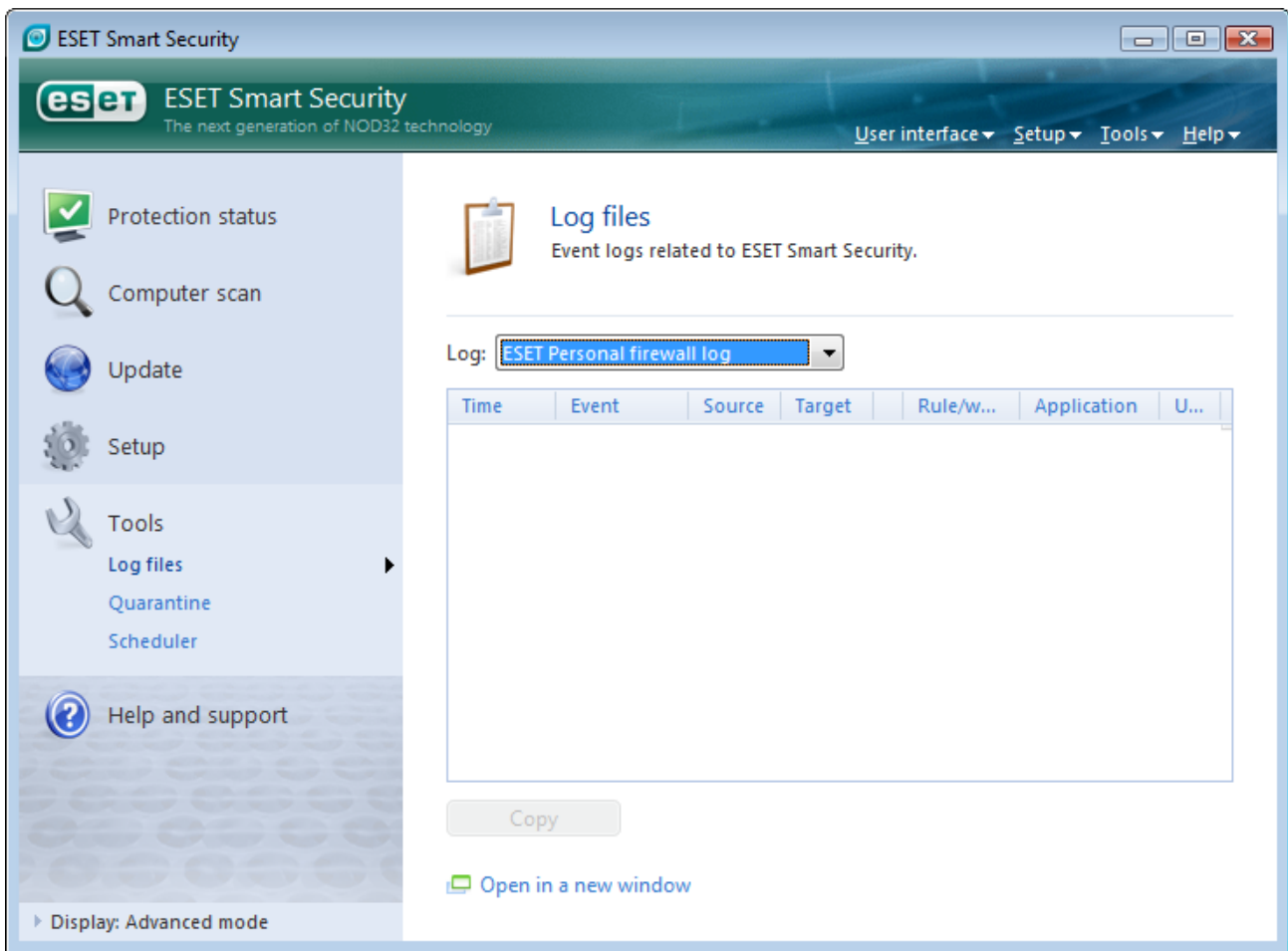
The modification detection feature also has its cons, but these can be alleviated through the use of exclusions. For example, a regular, legitimate upgrade to a newer version of Adobe Acrobat Reader may result in a process modification, since it automatically updates itself and downloads PDF documents from the Internet. Thus, a specific rule (exclusion) would need to be defined to allow this activity.

3.2 Logging network activity

Information about processed or blocked activity can be saved to a log and analyzed. Logging can be useful in determining why the Personal firewall blocked a certain communication. Press F5 to display the Advanced Setup window and then click **Personal firewall > IDS and advanced options** and select **Log all blocked connections**. Use the same dialog window to configure the IDS (Intrusion Detection System) as well as other general options (**Allow file and printer sharing in the Trusted zone, UPnP, etc.**).

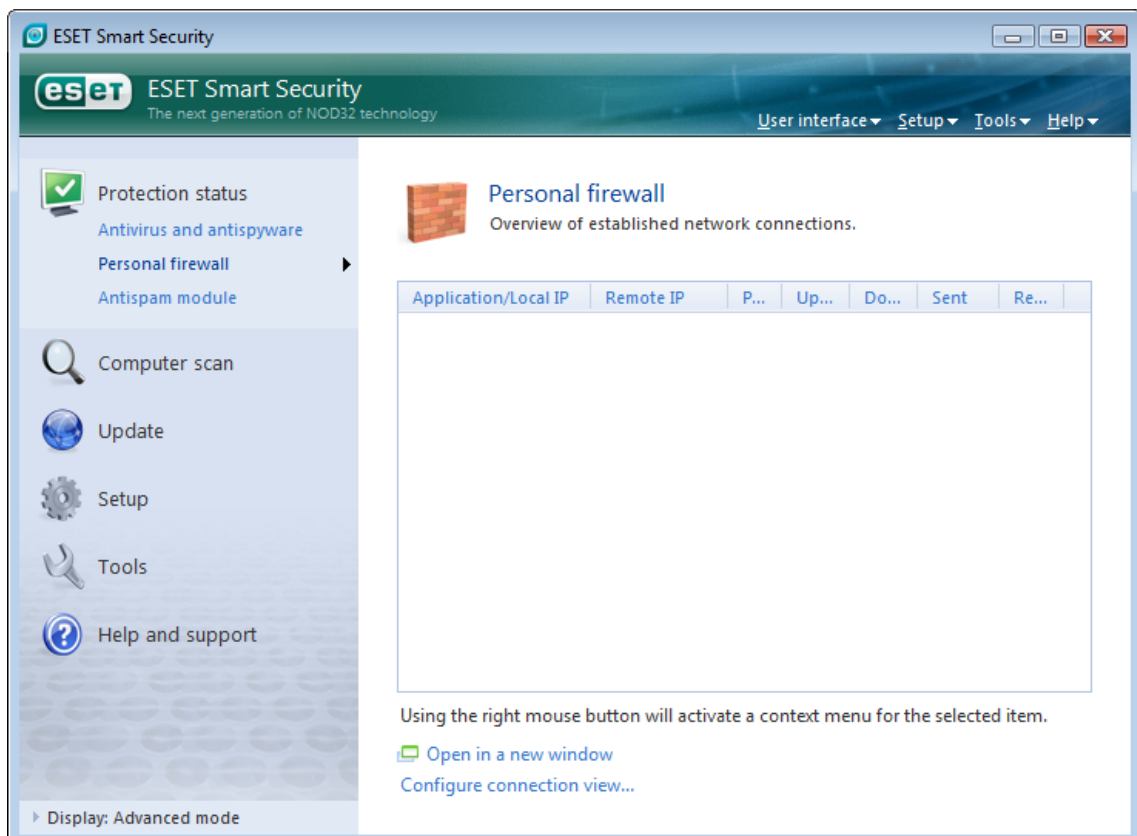


To find the reason for a blocked communication look in the Personal firewall log by clicking **Tools > Log files > ESET personal firewall log**. The most important information is under **Rule/worm name**, where you can often find the name of a rule that's disrupting communication.



Similarly, you can enable logging for any user-defined rule in the Personal firewall by selecting the **Log** option in the **New rule: window (Zone and rule setup window > New)**.

The current status of the Personal firewall can be viewed by clicking **Protection status > Personal firewall** from the main program window. You can right-click to open a context menu showing additional options, such as **Temporarily deny communication for a current process or connection**. If this option is chosen, a temporary rule bound to the PID of the process is created. When the process (application) terminates, the temporary rule is discarded.



3.3 XML Configuration files & ESET Configuration Editor

The ESET Configuration Editor is included with ESET Remote Administrator and can read configuration files exported by ESET Smart Security (for more information, see the ESET Remote Administrator manual). These configuration files also include rules and detailed configuration settings from the Personal firewall. The Personal firewall settings can be found in the Configuration Editor's tree structure under **ESET Smart Security, ESET NOD32 Antivirus > Personal firewall > Setup**.

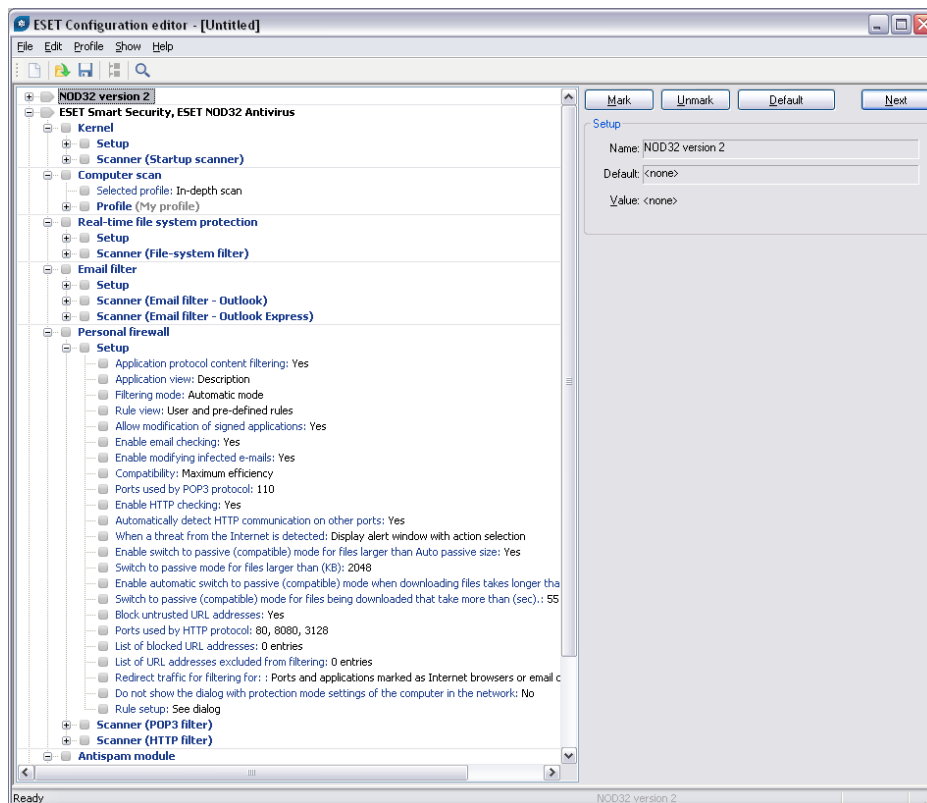
The most important attributes in the **Personal firewall > Setup** section are **Filtering mode** and **Rule setup**. These attributes allow you to specify rules, zones and other parameters. This dialog window looks almost the same as the one above, except for the option **Discard previous settings on the target computer**. If this option enabled, all current rules on the target computer will be removed and replaced by those in ESET Remote Administrator. If disabled, original rules will not be deleted or modified by new rules.

Warning! User-defined rules are identified by name. If the option **Discard previous settings on the target computer** is not enabled and an existing user-defined rule is renamed, a duplicate rule is created after the configuration is applied.

If you want to use an exported configuration but want to change Personal firewall settings only (and you do not wish to modify parameters of the real-time protection, email protection, update, etc.), the Configuration Editor offers the following methods:

1. Use the keyboard shortcut CTRL + D to remove blue icons in other settings (the icons will revert to grey).
2. Navigate to **ESET Smart Security, ESET NOD32 Antivirus > Personal firewall** and press SPACEBAR (the icon of every setting in the Personal firewall section will change to blue).
3. Save the configuration by clicking **File > Export selected to...**

The difference between blue and grey icons is described in detail in the ESET Remote Administrator manual. Essentially, any changes you make to settings in the ESET Configuration Editor are marked by a blue icon—the resulting .xml file will contain only these settings. If you were to push out the .xml configuration created using the steps above, only the Personal firewall settings would be modified on client computers³.



- 3 Remember that there are several methods of installing a new .xml configuration: as part of a configuration task in ERA, as a configuration assigned to a remote install package, or by using the Import feature directly from the ESET Smart Security user interface.

4. Summary

Let's summarize the most important points regarding deployment of the ESET Smart Security Personal firewall:

- The maximum level of protection is provided through Policy-based mode, though this method often requires fine-tuning of rules and zones.
- The ESET Personal firewall automatically blocks any communication which is not permitted by a rule. This is true for all modes except for Interactive filtering mode, which prompts the user to perform an action.
- If you are deploying the Personal firewall, we recommend that you configure at least one Trusted zone (Home network), regardless of the filtering mode. This will prevent users from seeing dialog windows asking them to add the current subnet to the Trusted or Not trusted zone.
- ESET Smart Security does not contain any predefined rules for handling communications within ESET Smart Security itself, as a security precaution. If you want to enable communication (updates, connection to ESET Remote Administrator Server, etc.), particularly in Policy-based mode, you must create corresponding rules.
- One of the most effective strategies for rule creation is to use Interactive filtering mode to automatically create rules through everyday interaction with the network. After all rules are specified, you can switch to Policy-based filtering mode, export the configuration to an .xml file and distribute it to other client computers.