SECURITY CODE

Secret Net Studio

Administrator's manual

Setup and operation. Network protection

Mailing address:	**P.O. Box 66, Moscow, Russian Federation, 115127**
Telephone:	**+7 495 982-30-20**
Email:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru/**

Table of contents

List of abbreviations

AD	Active Directory
FAT	File Allocation Table
IEEE	Institute of Electrical and Electronics Engineers
LFN	Long filename
MMC	Microsoft Management Console
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RPC	Remote Procedure Call
RTF	Rich Text Format
TCP	Transmission Control Protocol
USB	Universal Serial Bus
AWP	Automated Workplace
DB	Database
AEC	Application Execution Control
IC	Integrity Control
LDB	Local Database
DM	Data Model
OS	Operating System
CDB	Central Database

Introduction

This manual is designed for Secret Net Studio administrators (hereinafter "Secret Net Studio, the System"). It contains information for administrators about the configuration and management of the following protection mechanisms:

- personal firewall;
- network authentication.

Before reading this manual, read the following documents: [**1**], [**3**].

Conventions

In order to highlight certain elements in the text, a series of conventions is used.

Internal links usually indicate the required page number.

Important and additional information in the document is presented as notes. Icons in the margins indicate the importance of the information they contain.

- This icon highlights additional information that may contain examples, links to other documents, or other parts of the manual.

- This icon highlights important information that must be taken into account.

- This icon highlights a warning.

Exceptions. Some notes may not have any icons. Apart from note icons, the margins may also contain other graphical elements, for example, buttons that are explained in adjacent paragraphs.

Other information sources

If you have Internet access, you can visit SECURITY CODE Ltd. website (https://www.securitycode.ru/) or contact a company's representatives via email (info@securitycode.ru).

Chapter 1
General information

The Secret Net Studio network protection includes the following subsystems:

- firewall;
- network connection authorization mechanism.

Firewall

The firewall protects servers and workstations in the local area network against unauthorized access and controls network access.

The protection mechanism filters traffic at network, transport and application layers according to specified traffic filtration rules.

The firewall performs the following functions:

Function	Description
Network traffic filtering	Network traffic filtering is based on special rules with extensive settings. Network connections can be restricted at the following levels: • users; • computers; • user groups; • connection settings: service and application protocols, ports, network interfaces, applications, weekdays, time of day
Learning mode	With learning mode enabled, all network traffic is allowed. For each packet the system checks for a filtering rule that is configured in the firewall; default rules are excluded from the procedure. Several rules of the same type are grouped and replaced with a single rule

Network connection authorization mechanism

Secret Net Studio has a network protection mechanism implemented for authorized subscribers. This mechanism operates based on the IPsec framework of open standards and ensures data exchange security.

Subscriber authorization is based on the Kerberos protocol. This protocol is highly resistant to Man-in-the-middle attacks and password interception attempts. This mechanism provides authorization of access subjects as well as secure objects. This prevents unauthorized imitation of a secure information system, used in certain attacks.

The network connection authorization mechanism performs the following functions.

Function	Description
Network authorization	Adds service data to network packets that meet rules acquired from the control and authorization server. Analyzes incoming packet service data along with the transfer of information to the firewall module to ensure rule-based filtering
Inalterability control for transferred network packets	Ensures authenticity, integrity and confidentiality of transferred data
Traffic encryption	Ensures cryptographic protection of network traffic

Chapter 2
Firewall

You can configure the firewall centrally using the Control Center. Configuration is performed at the Computer object level, separately for each protected computer.

Note. Secret Net Studio also contains the Local Control Center component. This component only allows you to view firewall settings on a protected computer.

To configure the firewall:

1. Open the Control Center.

   The main program window appears.

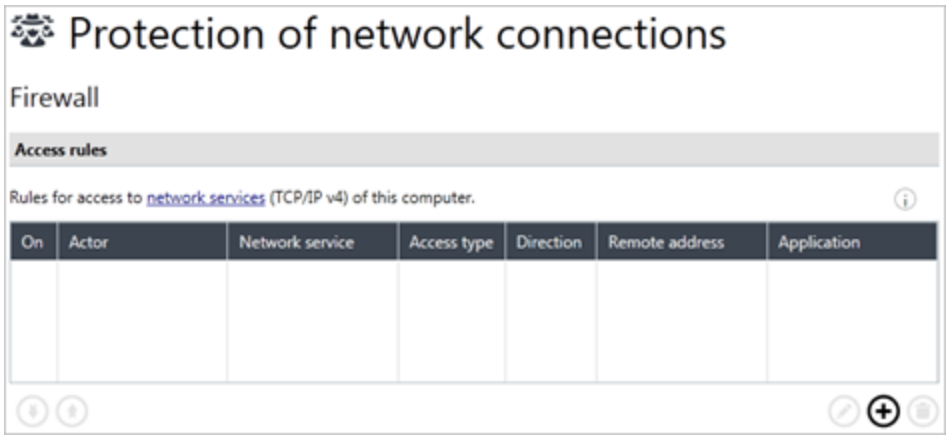
   Tip. To view firewall settings directly on a protected computer, open the Local Control Center, select the Settings tab, and select the Firewall element in the Policies section. Parameters cannot be configured in the local mode.

2. Open the Computers view on the left side of an open window and; select the computer you need, right-click the selected item, and then click Properties on the shortcut menu.

   An information about the computer status appears on the right side of the window.

3. Click the Settings tab and select the Firewall element in the Policies section.

   Interface of firewall configuration appears in the middle of the window as in the figure below.



4. Configure the parameters required and click the Apply button to save changes.

Network packet processing procedure

The Secret Net Studio network packet processing procedure depends on traffic direction.

- Incoming packets are first checked for compliance with network protocol settings; then, for compliance with system rules and then, if a packet passes the previous stages, it is checked for compliance with access rules;
- Outgoing packets are first checked for compliance with access rules; then, for compliance with system rules and then, if a packet passes the previous stages, it is checked for compliance with network protocol settings.

By default, object access rules are processed based on the order of their creation and position in the table of rules. The rules at the top of the table have the highest priority. (see p. 8).

If network packet properties match its description in a rule, a predefined action is performed. If access is denied, the packet is not checked for compliance with the rest of

the rules. If access is granted, the packet compliance check is continued. Network packets that are not subjects to any of the rules pass through the firewall.

Note. Service rules enabling network traffic necerequired for the Secret Net Studio to functioning are applied even when a packet was blocked at the previous stages.

Packet processing procedure for application rules:

- first, packets are processed according to the incoming traffic processing procedure;
- once the data is converted via operation with folders and named pipes, compliance with application rules is checked;
- once operations with folders and named pipes, as well as further conversion of a response into outgoing packages is complete, the corresponding processing procedure (outgoing packet processing) is performed.

If these operations are performed by a protected computer, it is not required to check for compliance with application rules.

Managing rule priority

By default, object access rules are processed based on the order of their creation and position in the rules table. The rules at the top of the table have the highest priority.

With the Secret Net Studio you can change rule processing priority.

To change rule priority:

1. From the list, select the rule.
2. To change the rule priority, click the Up or Down button.

Configuring access rules

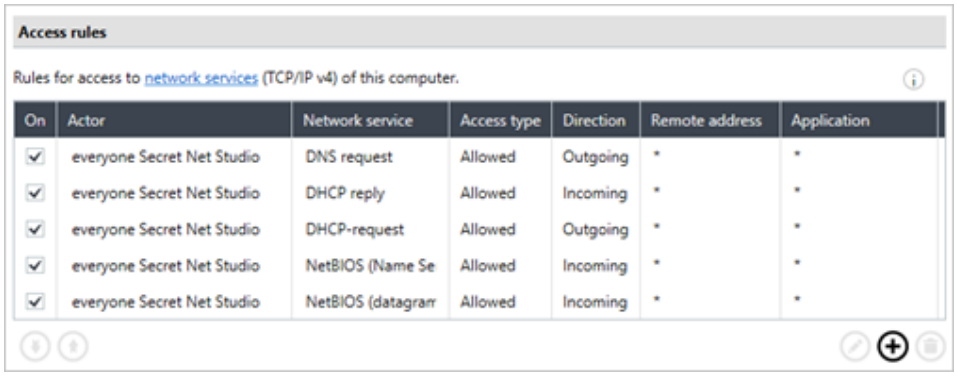
Access rules govern access for authenticated and anonymous users to the network services of a protected computer. These rules have higher priority than the application rules (see p. 19).

Attention!

- By default, the access rules govern all computer network interfaces.
- Changes to the rule settings take effect within 4-6 minutes.

To manage the rules:

1. Go to the Access rules section in the interface of the firewall configuration.



For each rule, the following information is displayed in the table:

Column	Value
On	Rule operation management: • unselected — the rule function is temporarily suspended • selected — the rule is enabled;
Actor	Name of the account or account group the rule applies to

Network service	Name of the network service the rule applies to
Access type	Type of access to a protected computer: • allowed; • denied
Direction	Network traffic direction the rule applies to
Remote address	Name or IP address of the computer the rule applies to. An asterisk (*) symbol indicates that the rule applies to all remote computers
Application	Path to the application that the rule applies to

2. Perform the required operations:
   - create a rule (see p. **9**);
   - edit rule properties (see p. **14**);
   - delete the rule (see p. **15**);
   - assign rule priority (see p. **8**);

Creating an access rule

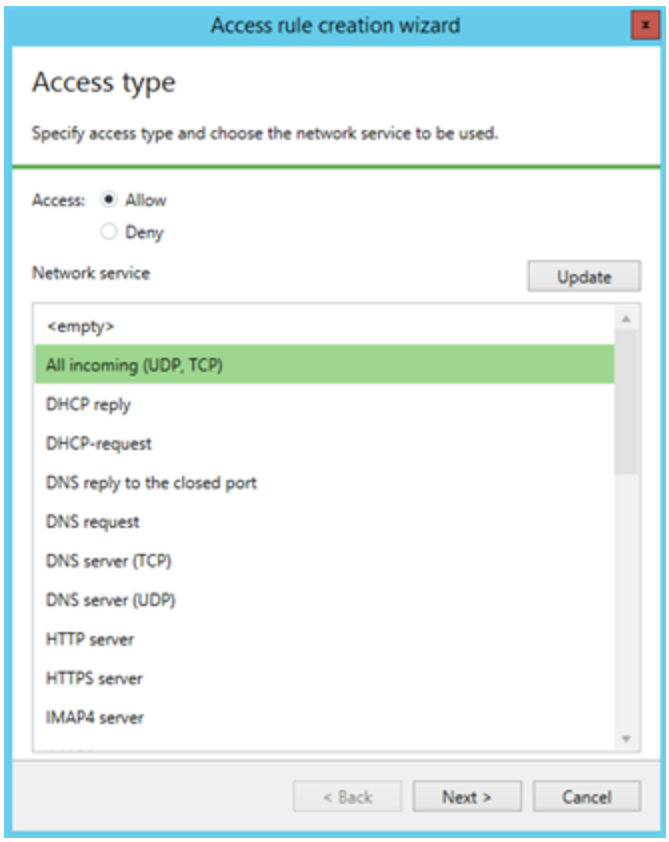
There is a special wizard for creating rules.

Tip. Use the buttons below to manage the rule creation procedure:
- < Back — to return to a previous dialog box;
- Next > — to proceed to the next dialog box;
- Cancel — to stop creating a rule.

To create an access rule:

1. Click the Add button.

   Access rule creation wizard appears.

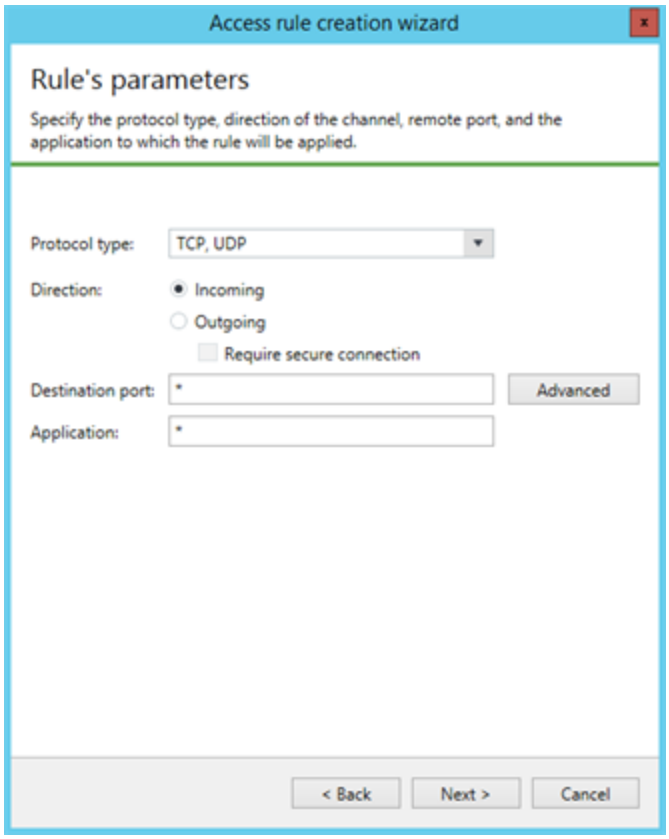


2. Specify the parameters and click the Next > button.

Section	Value
Access	Click the button: • Allow — if it is necessary to grant access to a protected object when a rule is triggered; • Prohibit — if it is necessary to deny access to a protected object when a rule is triggered
Network service	Select the name of a network service the rule applies to rule. Select the <empty> value to define network service parameters manually

Note. The network services list shows the services that are set by default. To display manually created services (see p. 30), click the Update button.

A dialog box appears as in the figure below.



3. Specify the required parameters and click the Next > button.

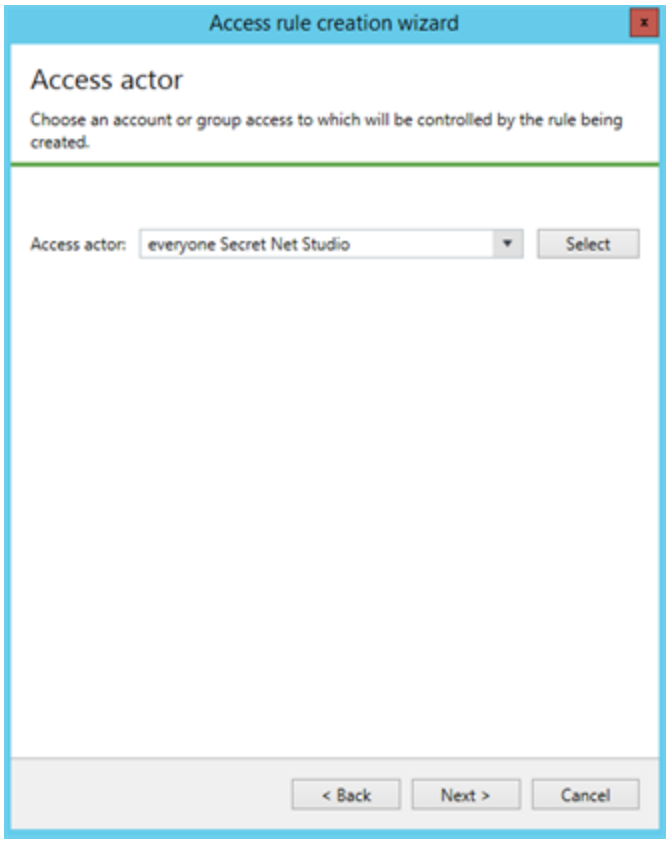
Section	Value
Protocol type	Select a protocol type the rule applies to
Direction	Select traffic direction that is subject to the rule (regarding a protected object)
Require secure connection	Select the check box if an outgoing network connection requires a secure data transfer channel
Destination port	Type the number of the port that is subject to the rule: • leave an asterisk (*) symbol if the rule must govern all computer ports sender or recipient of IP packets; • for incoming traffic, specify the port number for the IP packet receiving computer; • for outgoing traffic, specify the port number for the IP packet sending computer. Click the Advanced button to configure port range for a protected server or a remote computer

Section	Value
Application	Type the path to the executable file of an application subject to the rule: • specify the path to an application. You can also use Windows system variables to specify the path to an application; • leave an asterisk (*) symbol if the rule must govern all applications. A created rule will analyze network traffic for an application that operates directly on a protected computer

Attention! To ensure the access rule works properly, you must to specify the full path to the application's executable file.

Attention! While using the "Require secure connection" parameter, network connections are not be established through a not secure channel (if a license to use the network connection authorization mechanism is available).

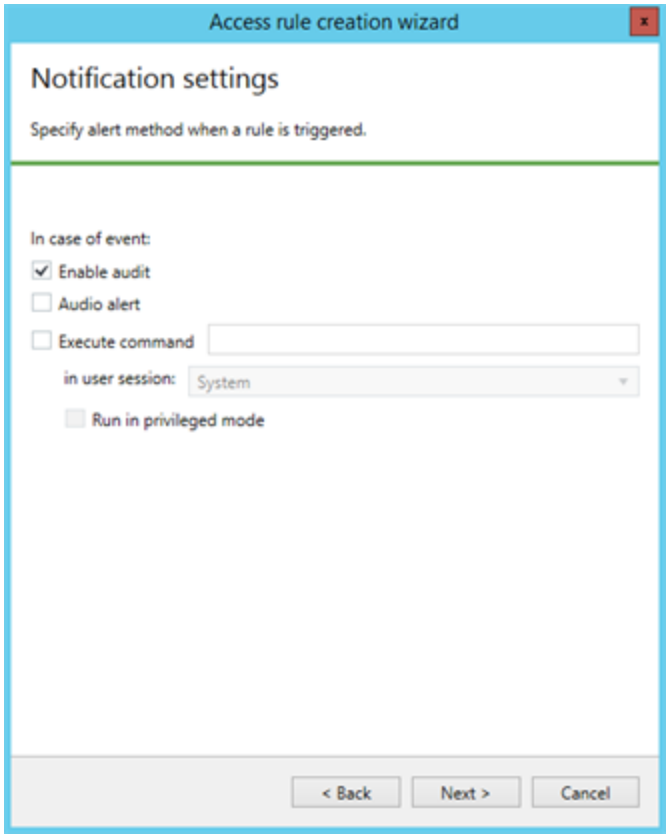
The Access actor dialog box appears.



Click the Select button to select accounts through the standard Windows dialog box. This function is available if you have a license to use the network connection authorization mechanism.

4. Specify the name of the account or account group to be governed by the rule and click Next > button.

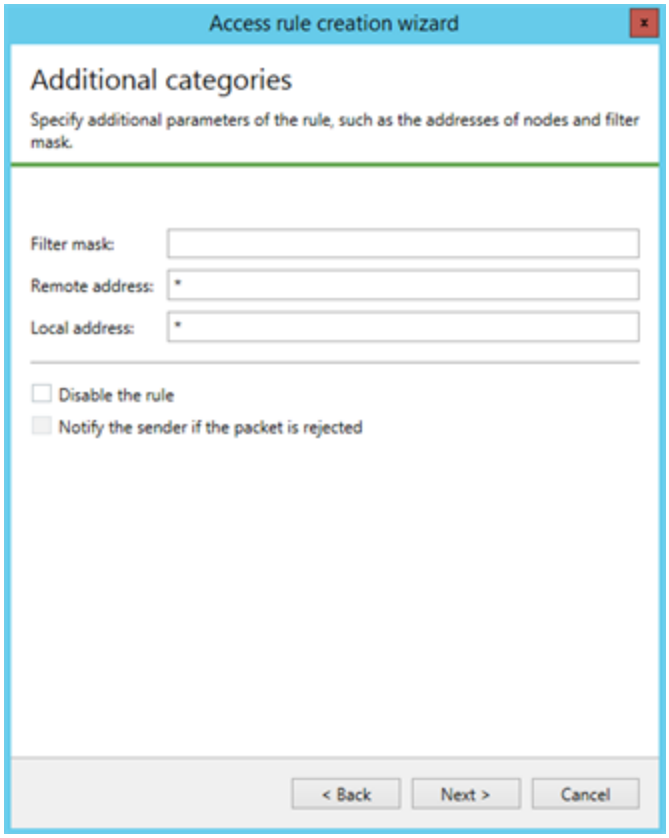
   The Notification settings dialog box appears.



5. Define the rule triggering alert methods and click Next > button (If necessary).

Section	Value
Enable audit	Select this check box to log the event when a rule is triggered. If event logging is not required, clear this check box
Audio alert	Select this check box if an audio alert is required to notify that a rule has been triggered on a protected computer. If audio alerts are not required, clear this check box
Execute command	Select this check box to run an executable file automatically when a rule is triggered. In the text box, which becomes available when the check box is selected, type the full path and the executable file name (with a parameter). For example, C:\windows\notepad.exe 1.txt
in user session	The field becomes available once the "Execute command" check box is selected. Select the user session where the specified command should be executed. • System — execute the command with system permissions; • Console — execute the command on behalf of a user during the user's session; • All user sessions — execute the command during all user sessions.
Run in privileged mode	Select to execute the command with full user permissions, even if User Account Control (UAC) is enabled for the user.

The Additional categories dialog box appears.



6. Specify the additional parameters for the rule and click Next >.

Section	Value
Filter mask	Type a value to define the need for processing an IP packet. If the box is filled in, the rule only concerns those IP packets with contents matching the filter mask. This box supports the following special characters: • * — for any number of characters; • ? — for a single character. For example, the value *abcd* will match any packet whose body contains the sequence abcd
Remote address	To define a suitable set of remote addresses, type a computer name, IP address, IP address range (e.g., 192.168.0.3-192.168.0.9) or a subnet (e.g., 192.168.1.0/24 or 10.10.0.0/255.255.0.0)
Local address	Type a computer name, IP address, IP address range or a subnet to define a suitable set of local addresses
Disable the rule	Rule operation management: • unselected — the rule is enabled; • selected — the rule function is temporarily suspended
Notify the sender if the packet is rejected	Managing notifications about packet blocking caused by the functioning of a blocking rule: • unselected — the sender does not receive notifications about blocked packets; • selected — the sender receives notifications about blocked packets. If a rule is triggered, RST packets will be generated for a TCP protocol, while ICMP packets (type: Destination Unreachable) will be generated for the other protocols (excluding ICMP, AH, ESP)

Tip. Leave an asterisk (*) symbol in the Remote address or Local address boxes for the rule to govern any addresses.
Use a semicolon (;) to separate multiple IP addresses, address ranges or subnets.

Note. The "Notify the sender if the packet is rejected" check box can be modified for rules with "Prohibit access" type access and "Incoming" traffic direction.

The Rule application schedule dialog box appears.

7. If necessary, configure the rule application schedule and click Finish:
   - select the Schedule check box. A table enabling schedule configuration becomes available;
   - click to choose weekdays and times for the rule application to be allowed (active rule) or blocked (inactive rule).

Note. The time when the rule is applied is defined by the time zone set on the protected computer.

The rule will be created and displayed in the list of rules.

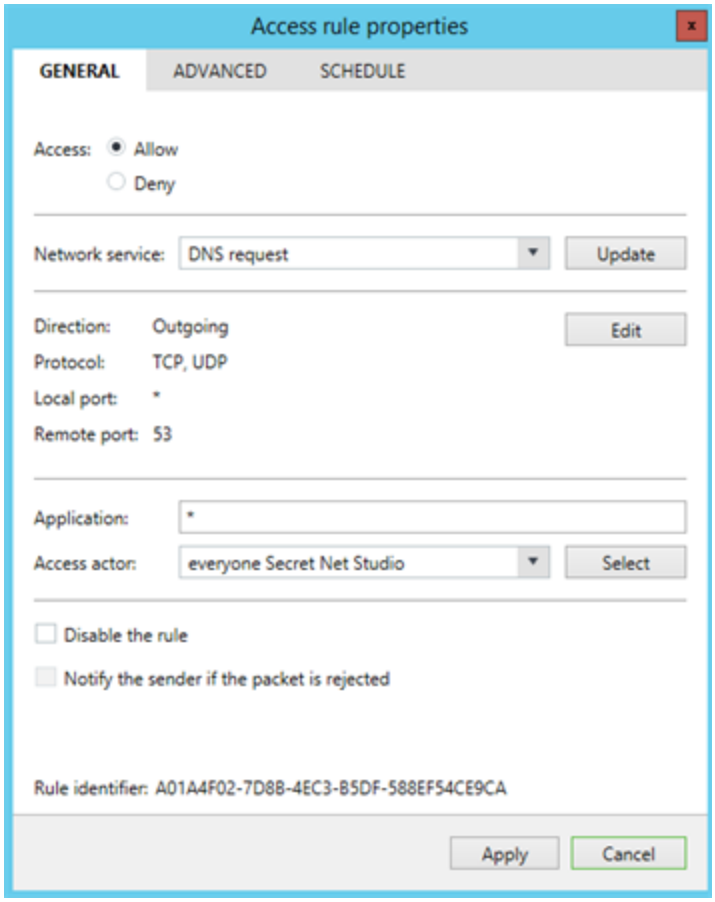
Managing access rules

Access rule parameters defined during its creation can be changed.

To change rule parameters:

1. In the table, select an access rule.
2. Click the Edit button.

   The Access rule properties dialog box appears.



Rule parameters in this box are the same as those described in the rule creation procedure.

3. To manage a rule:
   - select the "Disable the rule" check box to suspend the rule. The rule will be disabled;
   - clear the "Disable the rule" check box to restore the rule. The rule will be enabled.
4. Specify the required parameter values and click the Apply button.

Attention! If a rule that blocks service protocols (DNS, DHCP, etc.) was created by mistake, connection with the remote computer agent may be lost. In this case, the rules must be deleted using the Control Center (see below); then, run the following command on the protected computer as the local administrator:
C:\Program Files\Secret Net Studio\Client\Components\Network Protection\ScAuthModCfg.exe /r

Deleting an access rule

To delete an access rule:

1. Select the rule.

   Tip. Use the <Ctrl> and <Shift> keys to select multiple rules.
2. Click the Delete button.

   The selected rules will be deleted.

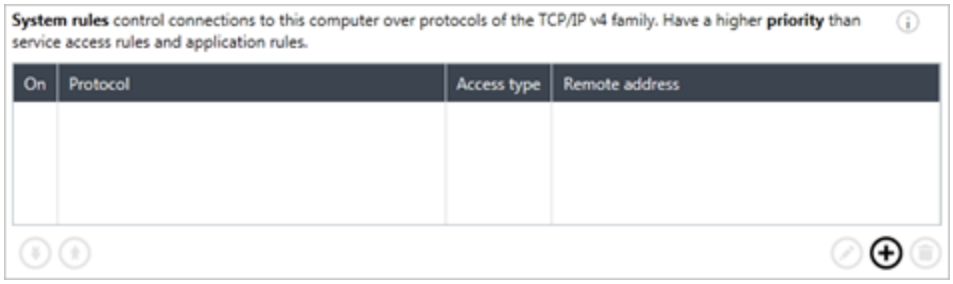
Managing system rules

System rules control connections with a computer via TCP/IP protocols. These rules have a higher priority than network service access rules and application rules.

To manage system rules:

1. Go to the Access rules section in the interface of the firewall configuration and click the Show specialized access rules link.

   A table containing the list of system rules appears.



   The following information is displayed for each rule:

Column	Value
On	Rule operation management: • unselected — the rule function is temporarily suspended • selected — the rule is enabled;
Protocol	Name of protocol subject to the rule
Access type	Type of access to a protected computer: • allowed; • denied
Remote address	Name or IP address of the computer the rule applies to, or asterisk (*) if the rule governs all remote computers

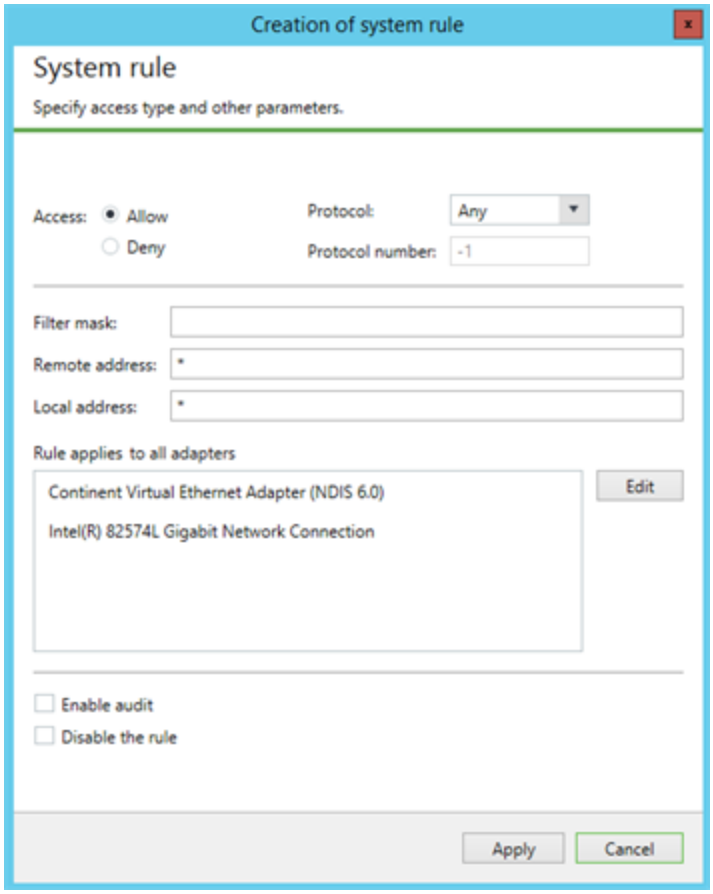
2. Perform the required actions:
   - create a rule (see p. **16**);
   - edit rule properties (see p. **18**);
   - delete the rule (see p. **15**);
   - assign rule priority (see p. **8**);
   - configure ICMP protocol protection mode (see p. **29**).

Creating a system rule

To create a system rule:

1. Click the Add button.

   The System rule dialog box appears.



2. Specify the rule parameters and click the Apply button.

Section	Value
Access	Click the button: • Allow — if it is necessary to grant access to a protected object when a rule is triggered; • Prohibit — if it is necessary to deny access to a protected object when a rule is triggered
Protocol	Select a protocol type subject to a rule: • Any — if a rule is needed to govern all protocol types; • Other — if the required protocol type is not in the list. In this case, the Protocol number box becomes available
Protocol number	If a protocol type is selected, this text box value is defined automatically and cannot be modified. If the Protocol list box has the value Other, type the number of the protocol subject to the rule
Filter mask	Type a value to define the need for processing an IP packet. If the box is filled in, the rule only concerns those IP packets with contents matching the filter mask. This box supports the following special characters: • * — for any number of characters; • ? — for a single character. For example, the value *abcd* will match any packet whose body contains the sequence abcd
Remote address	Type a computer name, IP address, IP address range (for example, 192.168.0.3-192.168.0.9) or a subnet (for example, 192.168.1.0/24 or 10.10.0.0/255.255.0.0) to define an allowable set of remote addresses. Leave an asterisk (*) character if the rule must be applied to all remote computers
Local address	Type a computer name, IP address, IP address range or a subnet to define a suitable set of local addresses. Leave an asterisk (*) character if the rule must be applied to all remote computers

Section	Value
Rule applied on all adapters	For the rule to govern only specific adapters, click the Edit button and select the adapters
Enable audit	Manage logging of events when a rule is triggered: • unselected — event logging is disabled; • selected — event logging is enabled
Disable the rule	Rule operation management: • unselected — the rule is enabled; • selected — the rule function is temporarily suspended
Notify the sender if the packet is rejectede	Managing notifications about packet blocking caused by the functioning of a blocking rule

The newly created rule will be displayed in the rules list.

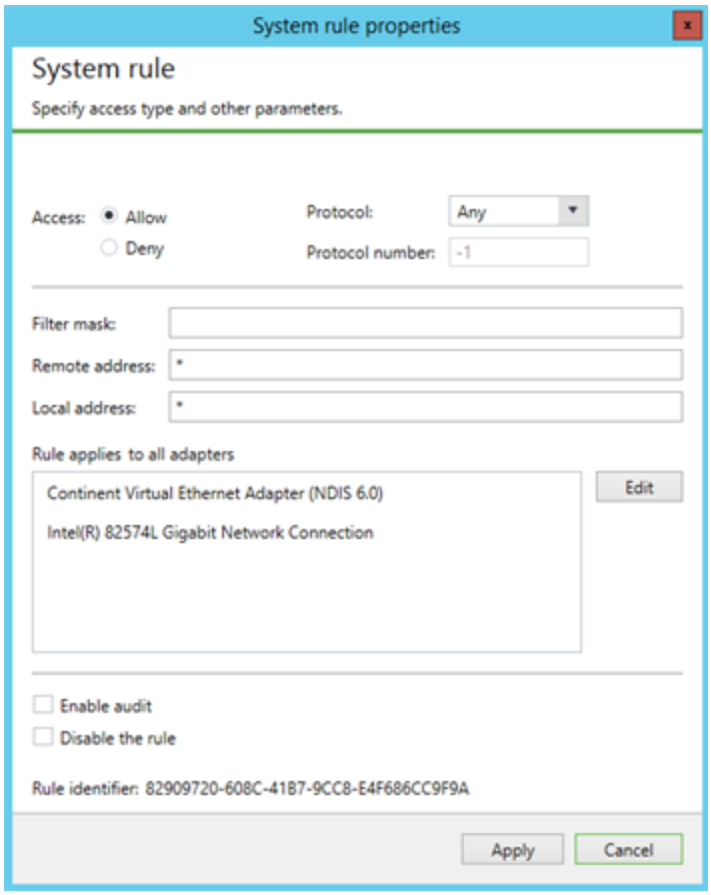
Managing system rules

The system rule parameters defined during its creation can be changed.

To change rule parameters:

1. In the table, select a system rule.
2. Click the Edit button.

   The System rule dialog box appears.



   Rule parameters in the configuration dialog box are the same as those described in the rule creation procedure.

3. To manage a rule:

- select the "Disable the rule" check box to suspend the rule. The rule will be disabled;
- clear the "Disable the rule" check box to restore the rule. The rule will be enabled.

4. Change the required parameter values and click the Apply button.

Managing application rules

Application rules govern access for authenticated and anonymous users to shared folders and named pipes on a specific computer. These rules have the least priority.

To manage the rules:

1. Go to the Access rules section in the interface of the firewall configuration and click the Show specialized access rules link button.

   A table containing the list of application rules displays.

   The following information is displayed for each rule:

Column	Value
On	Rule operation management: • unselected — the rule function is temporarily suspended • selected — the rule is enabled;
Actor	Name of the account or account group the rule applies to
Application service	Name of application service: • Shared folders; • Named pipes
Access object	Name of shared folder or channel subject the rule applies to. An * (asterisk) character indicates that the rule applies to all objects of this type
Access type	Type of access to a protected computer: • allowed; • denied
Remote address	Name or IP address of the computer the rule applies to. An asterisk (*) character indicates that the rule applies to all remote computers

2. Perform the required actions:
   - create a rule (see p. **19**);
   - edit rule properties (see p. **23**);
   - delete the rule (see p. **15**);
   - assign rule priority (see p. **8**);

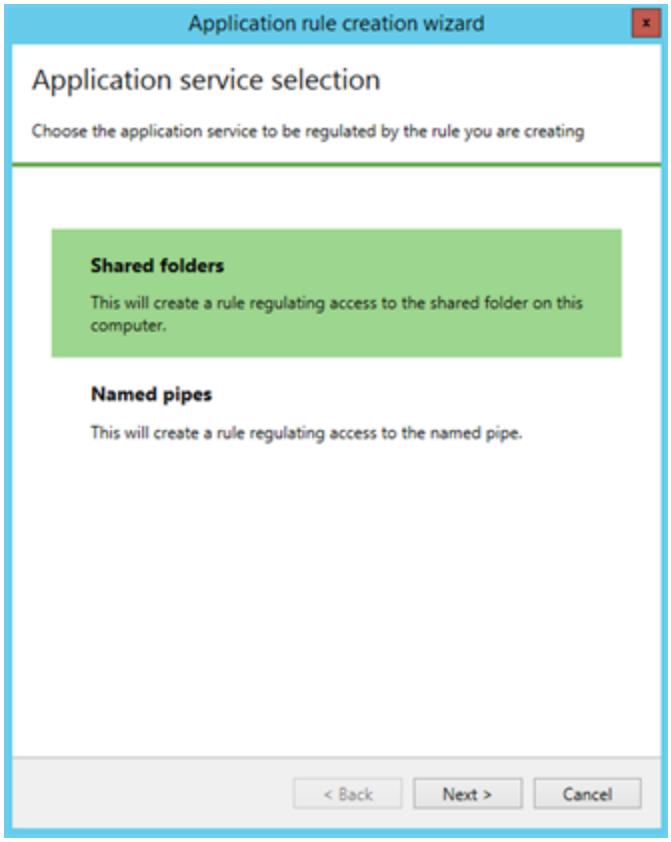
Creating an application rule

There is a special wizard for creating application rules.

To create a rule:

1. Click Add.

   The first dialog box of the rule creation wizard appears.

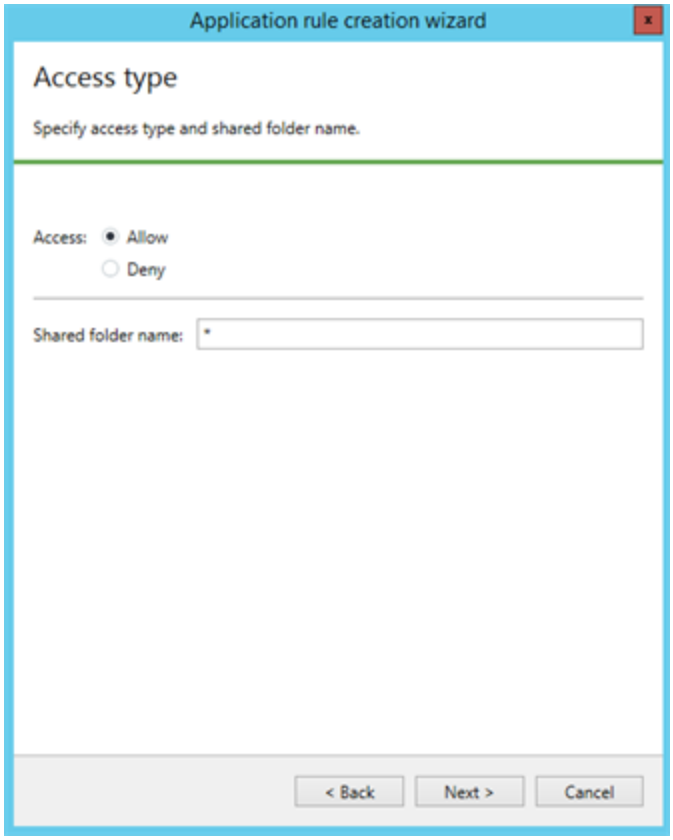


2. Select an application service for which you wish to create a rule and click Next >:

- Shared folders — the new rule will govern user access to a specified shared folder via SMB protocol;
- Named pipes — the new rule will govern user access to a specified channel via Named Pipes protocol.

Note. Application rules enable restricting user access to shared folders and their contents (for example, \\server\share). Granular access control to the subfolders of shared folders (for example, \\server\share\folder) is not provided.

A dialog box asking you to configure the rule parameters appears.



3. Define the parameters and click Next >.

Field	Value
Access	Select a value: • Allow — if it is necessary to grant access to a protected object when a rule is triggered; • Prohibit — if it is necessary to deny access to a protected object when a rule is triggered
Shared folder name/Named pipe	Specify the name for a folder or a pipe that is to be subject to the rule. Put an * (asterisk) character if the rule is to govern all folders or named pipes on this computer

- A shared folder name is specified without the name of the computer where it is located. For instance, if the path to the folder on the server is \\server\share, you only need to specify its name: share.
- The folder or pipe name may contain special characters: ? (question mark) to replace a single character, and an * (asterisk) to replace several characters, including an empty space.
- Should access to shared folders of a protected object be restricted for all users (i.e. a blocking rule governs the <everyone> account where the shared folder name is specified as an * (asterisk)), then, users who want to browse the list of shared folders on this computer have to create an allow rule for the IPC$ shared folder.

A dialog box asking you to select accounts governed by the rule appears.

Tip. Use the Select button to select accounts through the standard Windows dialog box.

4. Specify the name of the account or account group to be governed by the rule and click Next >.

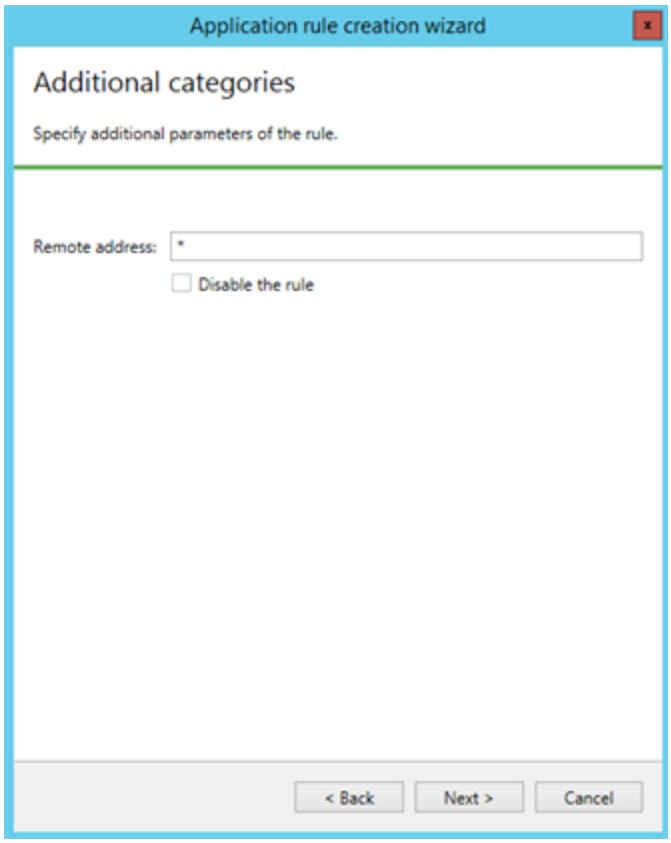
   A dialog box prompting you to configure rule triggering notifications appears.

5. If necessary, define the rule triggering alert methods and click Next >.

Field	Value
Enable audit	Select this check box to log the event when a rule is triggered. If event logging is not required, clear this check box.

Field	Value
Audio alert	Select this check box if an audio alert is required to notify that a rule is triggered on a protected computer. If audio alerts are not required, clear this check box
Execute command	Select this check box to run an executable file automatically when a rule is triggered. In the text field, which becomes available when the option is selected, enter the exact path and the executable file name (with a parameter). For example, C:\windows\notepad.exe 1.txt
in a user session	The field becomes available once the "Execute command" option is selected. Select the user session where the specified command should be executed. • System — execute the command with system permissions; • Console — execute the command on behalf of a user during the user's session; • All user sessions — execute the command during all user sessions.

The Additional categories dialog box appears.



6. Specify the additional parameters for the rule and click Next >.

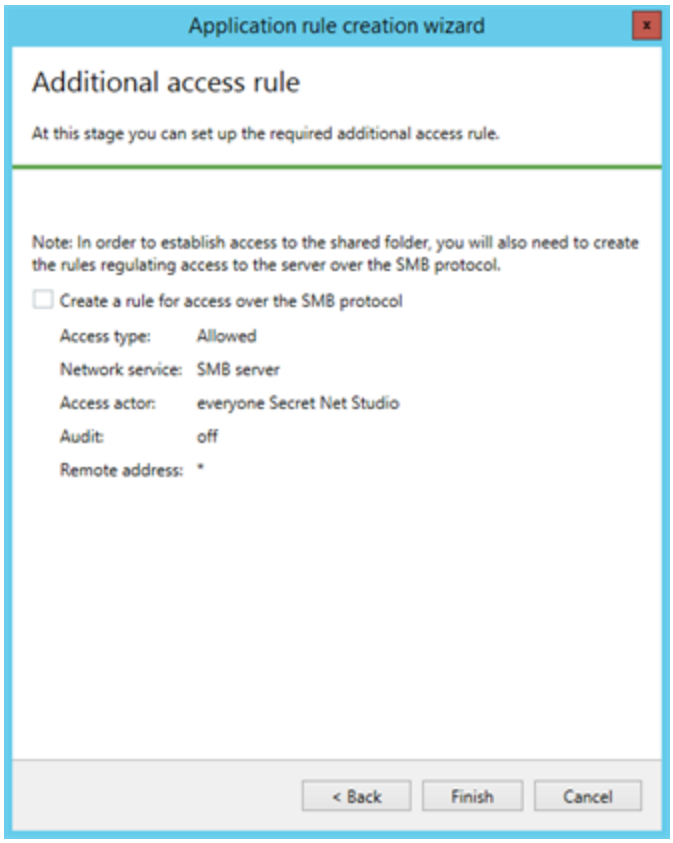
Field	Value
Remote address	Type a name or an IP address (subnet mask) for the computer that is to be governed by the rule when there is an attempt to gain access to a shared folder or a named pipe on the protected computer. Put an asterisk (*) character if a rule must govern all computers (IP packet senders)
Disable the rule	Select this checkbox to enable the rule later

The Rule application schedule dialog box appears.

7. Configure the rule application schedule, if necessary, and click Next >:
   - select the Schedule check box. A table enabling schedule configuration becomes available;

- click table cells to highlight weekdays and periods of time for the rule to apply (active rule) or not (inactive rule).

The Additional access rule dialog box appears.



For application rules to function properly, it is also necessary to configure the IP package pass-through rules at the transport level via SMB protocol. This also requires creating an access rule that allows packets to pass through via TCP protocol on port 445 (and/or 139) for an account (group) listed in the application rule.

Attention! If package pass-through via SMB protocol is blocked, application rules are disabled, because IP packets are blocked on the transport level.

8. If it is necessary to create an allow rule for the SMB protocol, select the "Create a rule for access over the SMB protocol" check box.
9. Click Finish.

   The new rule will be added to the list of application rules.

   When creating an additional SMB rule, the access rules list will also show the rule allowing an account (group) specified in an application rule to use SMB protocol.

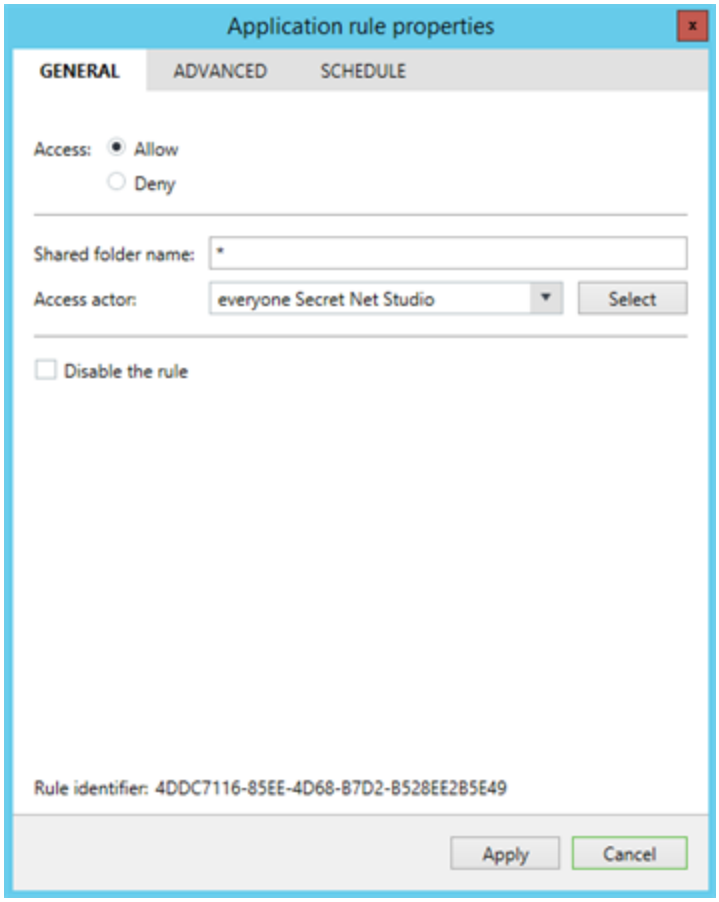
Managing application rules

The application rule parameters defined during its creation can be changed.

To change rule parameters:

1. In the table, select an application rule.
2. Click Edit.

   The Application rule properties dialog box appears.



Rule parameters in the configuration dialog box are the same as those described in the rule creation procedure.

3. To manage a rule:
   - select "Disable the rule" check box to suspend the rule. The rule will be disabled;
   - clear "Disable the rule" check box to restore the rule. The rule will be enabled.
4. Specify the required parameter values and click Apply.

Managing network traffic filtering rules

Network traffic filtering rules are designed to filter network protocol commands, command parameters and to control access to resources that contain certain mobile code types.

Network traffic filtration rules are managed by the command line utility ScAuthSrvConfig.exe (when Secret Net Studio in network mode) or ScLocalSrvConfig.exe (in stand-alone mode).

The ScAuthSrvConfig.exe utility can be found on the Security Server, in the setup folder Secret Net Studio\Server\Authentication Server\.

Note. To enter configuration management mode, the ScAuthSrvConfig.exe must be sent the parameters for connecting to the management server (see below).

The ScAuthSrvConfig.exe utility can be found on the protected computer in the setup folder Secret Net Studio\Client\Components\Network Protection\.

Attention! You must have local administrator rights to change local configuration via ScLocalSrvConfig.exe.

Connection to the management server

To enter configuration management mode, the ScAuthSrvConfig.exe must be sent the parameters for connecting to the management server. Open the command

prompt and run the following command:

```
ScAuthSrvConfig [@argfile] [/?|h|help] [/v|version] <domain>
[/local] [kdc] [/p|password <value>] [/a|admin <value>] [/q
<value>] [/s <value>]
```

where:

- @argfile — read arguments from file;
- /? — display detailed information about the utility;
- /v — display the utility version number;
- domain — Kerberos domain;
- /local — local mode (configuration recovery);
- kdc — the Key Distribution Center location;
- /p <value> — domain administrator password;
- /a <value> — domain administrator name;
- /q <value> — query execution command;
- /s <value> — path to the script file to be executed.

Example.

Connecting to the management server running on a used computer:

```
ScAuthSrvConfig.exe DOMAINNAME 127.0.0.1 /admin Administrator
```

where:

- DOMAINNAME — security domain;
- 127.0.0.1 — network address of the configuration server;
- Administrator — Secret Net Studio administrator name.

Creating and editing network traffic filtering rules

To add a new network traffic filtering rule, open the command prompt and run the following command:

```
config> add network_stream_filtration_rule(nsfr) <protected_
computer> /filter <value> [/flt-case-insensetive | /flt-case-
sensitive] [/at allow|deny] [/order <value>] [/local_addrs
<value>] [/local_ports <value>] [/remote_addrs <value>]
[/remote_ports <value>] [/direction <value>] [/audit 1|0]
[/enable 1|0]
```

The following rule parameters are available:

Parameter	Description	Available values
filter	Filter mask	• * — for any number of characters; • ? — for a single character.
flt-case-insensitive	Case insensitive search	
flt-case-sensitive	Case sensitive search Default value	
at (access type)	Access rule type	• deny — the connection will be terminated if a sequence that fits the filter mask is found. Default value; • allow — only audit (if allowed) will be performed if a sequence that fits the filter mask is found.

Parameter	Description	Available values
direction	The list of connection (network traffic) directions to which the rule will apply. ";" is used as a separator.	• in — the rule will be applied to incoming connections, incoming traffic. Default value; • in_reply — the rule will be applied to incoming connections, response traffic. • out — the rule will be applied to outgoing connections, outgoing traffic. • out_reply — the rule will be applied to outgoing connections, response traffic.
local_addrs	The list of local addresses/networks/ranges for which the rule applies. ";" is used as a separator.	
local_ports	The list of local ports/ranges for which the rule applies. ";" is used as a separator.	
remote_addrs	The list of remote addresses/networks/ranges for which the rule applies. ";" is used as a separator.	
remote_ports	The list of remote ports/ranges for which the rule applies. ";" is used as a separator.	
audit	Enable/disable audit when the rule is triggered	• 1 — audit is enabled; • 0 — audit is disabled;
order	Rule application procedure. The parameter only affects rule triggering.	
enable	Current rule status	• 1 — the rule is enabled; • 0 — the rule is disabled;

The following command is used to edit a filtering rule:

```
config> modify network_stream_filtration_rule(nsfr)
<protected_computer> <rule_id> [/filter <value>] [/at
allow|deny] [/order <value>] [/local_addrs <value>] [/local_
ports <value>] [/remote_addrs <value>] [/remote_ports
<value>] [/direction <value>] [/audit 1|0] [/enable 1|0]
```

where <rule_id> is the identifier of the rule to be modified.

Examples

Example 1. Single command filtering

Creating a rule to be applied to outgoing network connections through port 23. The rule is triggered when identified in the outgoing "cmd" command:

```
add nsfr SP-VM01 /filter "cmd1" /direction out /remote_ports
23
```

Example 2. Filtering a sequence of commands.

Creating a rule to be applied to outgoing network connections through port 23. The rule is triggered when a sequence of "cmd1", "cmd2" and "cmd3" commands is identified in outgoing data. Any number of characters can be between these commands.

```
add nsfr SP-VM01 /filter "cmd1*cmd2*cmd3" /direction out
/remote_ports 23
```

Example 3. Filtering a command parameter

Creating a rule to be applied to outgoing network connections through port 23. The rule is triggered when the "cmd" command with the "param" parameter is identified in outgoing data.

```
add nsfr SP-VM01 /filter "cmd*param" /direction out /remote_
ports 23
```

Example 4. Filtering access to resources that contain certain mobile code types

To filter access to resources that contain certain mobile code types, network traffic filtering rules are used. As a filter, these rules contain text sequences that are typical for a certain type of mobile code. For example, to prohibit a mobile code in the HTTP protocol, you will need to create rules for outgoing connections, for response traffic with filtering by "Content-Type" header. Extra filtering can be applied by checking the "Content-Disposition" heading and its "filename" parameter.

List of "Content-Type" headers for various mobile code types:

Mobile code type	Filtered string
JavaScript	Content-Type: text/javascript Content-Type: text/jscript Content-Type: text/x-javascript Content-Type: text/ecmascript Content-Type: text/x-ecmascript Content-Type: application/javascript Content-Type: application/x-javascript Content-Type: application/ecmascript Content-Type: application/x-ecmascript
Adobe Flash	Content-Type: application/x-shockwave-flash
VBScript	Content-Type: text/vbscript
Java	Content-Type: application/java-archive Content-Type: application/jar
ActiveX	Content-Type: application/ocx Content-Type: application/x-ms

An example of creating a set of mobile code filtering rules:

```
add nsfr SP-VM01 /filter "Content-Type: application/ocx"
/flt-case-insensitive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter "Content-Type: application/x-ms"
/flt-case-insensitive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter " Content-Disposition*filename*ocx"
/flt-case-insensitive /direction out_reply /remote_ports 80
```

The rules block loading Active-X components via HTTP protocol, port 80.

Viewing network traffic filtering rules

To view the list of network traffic filtering rules, run the following command:

```
config> show network_stream_filtration_rules(nsfrs)
<protected_computer>
```

where <protected_computer> is the protected computer name.

Example.

```
config> show nsfrs SP-VM01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
direction out
proto 6
local-addr *(*)
remote-addr *(23)
```

Use the following command to view detailed information about an individual rule for filtering network traffic:

```
config> show network_stream_filtration_rule(nsfr) <protected_
computer> <id>
```

where:

- <protected_computer> is the protected computer name.
- <id> — rule identifier.

Example.

```
config>show nsfr SP-VM01 {ca541ade-b955-4cf2-8894-
d020aac9d9ac}
server: sp-vm01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
enabled 1
direction out
proto 6
local-addr *(*)
remote-addr *(23)
audit 1
```

Deleting network traffic filtering rules

To delete a network traffic filtering rule, run the following command:

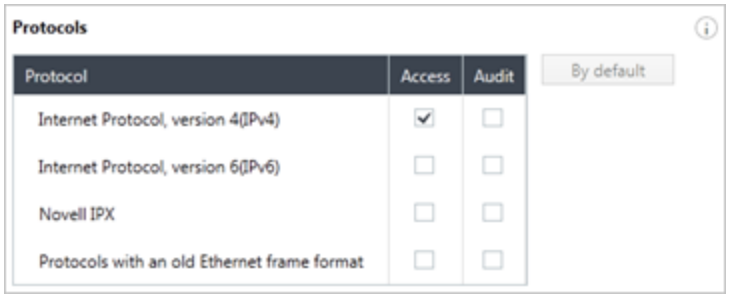
```
config> delete network_stream_filtration_rule(nsfr)
<protected_computer> <id>
```

Managing network protocols

The Secret Net Studio configures access to protected computers via IPv4, IPv6, Novell IPX network protocols, as well as other protocols with older Ethernet frame format (LLC, IPX). These protocols, apart from IPv4, are blocked by default. These settings have a higher priority than network service access rules, application rules and system rules.

To manage network protocols:

1. Open the Protocols section on the interface of the firewall configuration.



2. In the Access column, clear the check boxes to disable protocols. Select the check boxes to enable these protocols.

Attention! By default, access to protected computers is only granted via the IPv4 protocol. It is not recommended to enable other protocols, as the traffic will not be monitored by the Secret Net Studio firewall.

3. In the Audit column, select the protocols for which events must be logged for every packet that passes through. If event logging is not required, clear this check box.

   The audit (event logging) mode for all protocols is disabled by default.

Attention! When audit mode is enabled, the number of events logged by Secret Net Studio will be very big. This may cause the system to slow down.

Comment. The Audit check box value in the protocol settings is not associated with the Enable audit value specified in the access rule properties.

4. To save the new parameter values, click the Apply button in the top of the Settings tab.

Tip. Use the By default button to restore the table's original version.

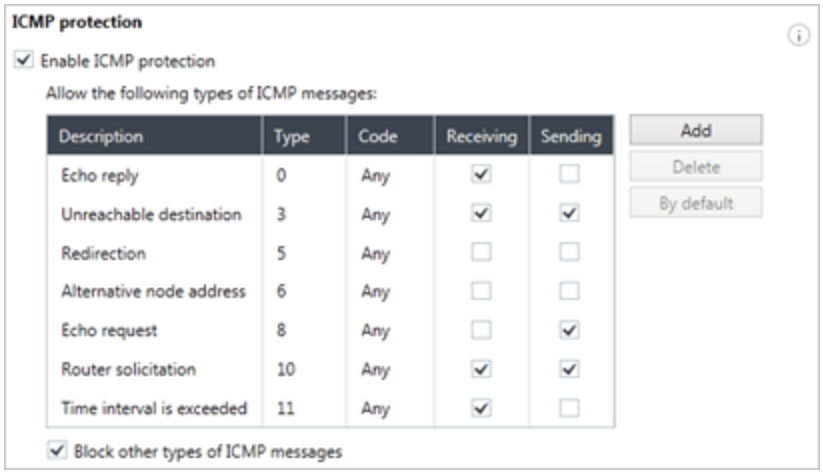
The Protocols with old Ethernet frame format option makes it possible to block Ethernet frames which contain a frame value in the heading instead of its type. Through such frames, IPX, SMB over NetBEUI and event IP traffic can reach the protected server.

Configuring ICMP protocol protection mode

The ICMP protocol protection mode is used to exchange messages via this protocol. The ICMP protocol packet management mode is disabled by default.

To configure mode parameters:

1. Go to "ICMP protection" section in the interface of the firewall configuration.



   ICMP protocol packet types are shown as a table. The following information is displayed for each type:

   - packet type description;
   - packet type;
   - packet code;
   - means to manage packet pass-through.

2. Configure the necessary parameters.

Parameter	Value
Enable ICMP protection	Select this check box if it is necessary to enable ICMP protection

Parameter	Value
Receiving and Sending columns	Allow or prevent incoming and outgoing packets to pass through. To allow, select the corresponding check box; clear to prevent it
Block other types of ICMP messages	Select this check box to prevent all ICMP packet types passing through, except for the types specified in the table. If you need to allow packets to pass through, clear the check box

Tip. Use the buttons on the right to add ICMP message types (Add), delete added rows (Delete) or restore the table to its default settings (By default).

3. To save the new parameter values, click the Apply button in the top of the Settings tab.

   ICMP protocol packet processing mode will be configured according to the specified parameter values.

Managing network services

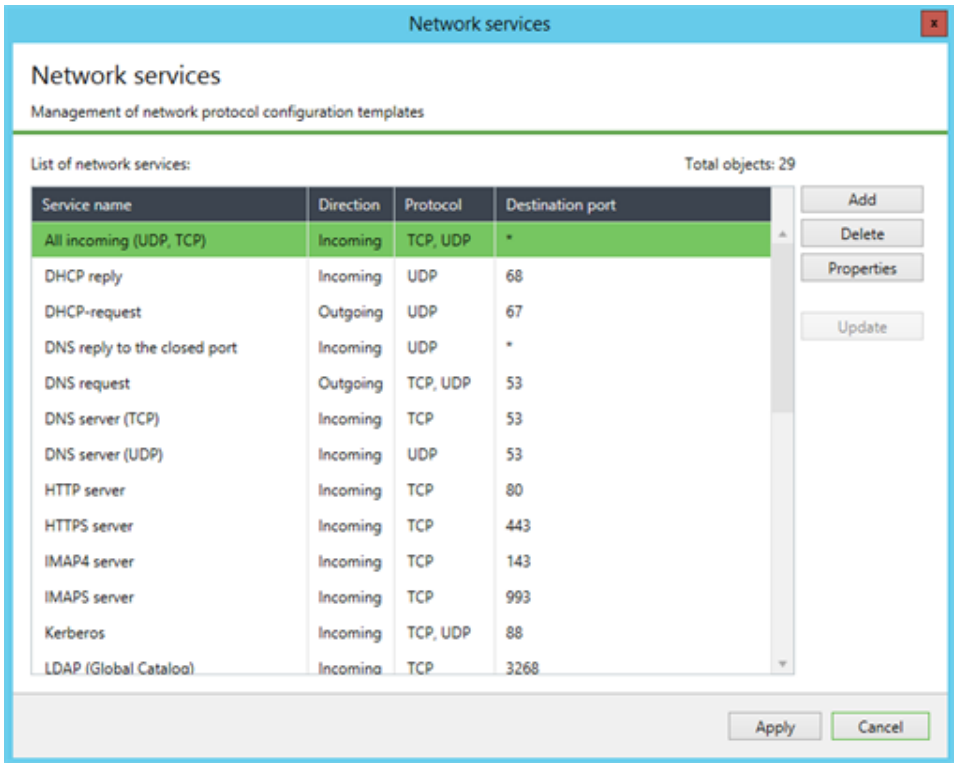
Network services are a list of the most common network protocol templates. The following information is displayed for each service:

- network service name;
- traffic direction governed by the network service;
- network service protocol type;
- computer port governed by the network service.

To manage network services:

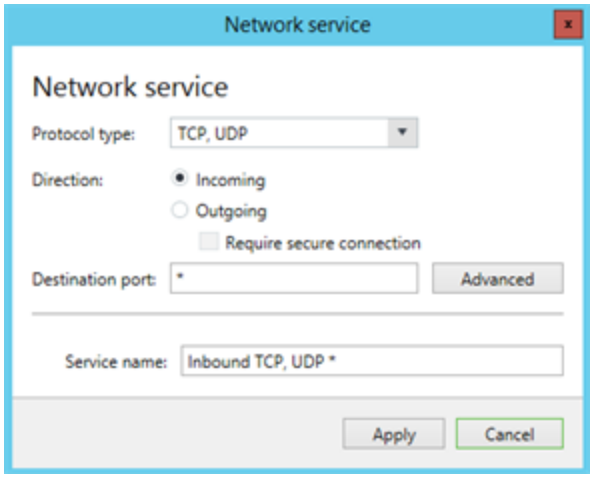
1. Click the "network services" link in the Access rules section of the firewall configuration interface.

   The Network services dialog box appears.



2. To create a network service, click the Add button.

   The Network service dialog box appears.



3. Specify the required parameters and click the Apply button.

Field	Value
Protocol type	Select the type of protocol governed by the network service
Direction	Click one of the buttons to specify a traffic direction governed by the network service: • Incoming; • Outgoing
Require secure connection	If a secure connection is required when the network service is in use, select this check box (see p. **34**)
Destination port	Type the number of the port governed by the network service: • put an asterisk (*) character if a service governs all computer ports (IP packet sender or recipient); • for incoming traffic, specify the port number for the IP packet receiving computer; • for outgoing traffic, specify the port number of the IP packet sending computer; To specify a destination port range, use the Advanced button next to the Destination port text box and enter the port range in the pop-up dialog box
Service name	Enter a name for the network service template to be saved

A network service will be created and displayed in the network service list.

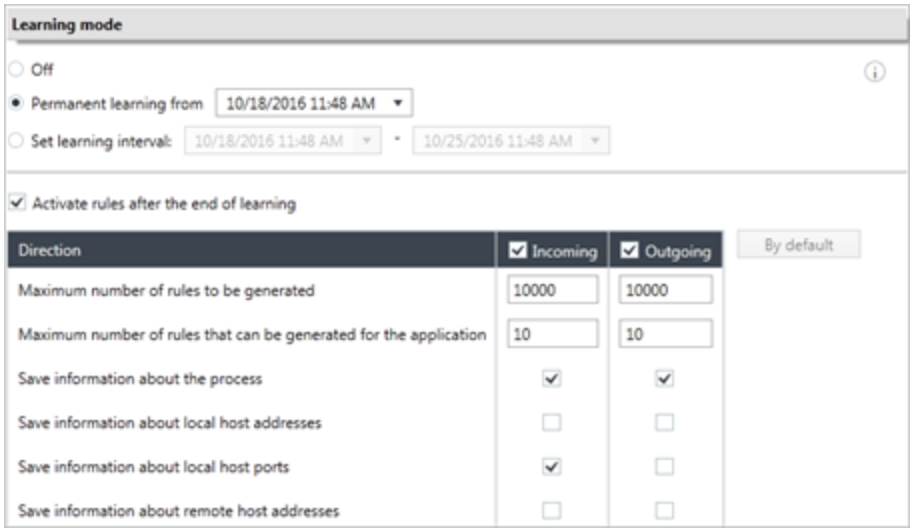
4. To delete a single or multiple network services, select the service(s) and click Delete. The selected network services will be deleted.
5. To modify the parameters of a network service, select the required one from the list and click the Properties button. In the pop-up window, change the required service parameters based on the description in step **3** of this procedure.

Configuring learning mode

The learning mode is used when launching the protection system stage. This mode allows a base set of access rules to be composed that are required for the protected computer to function. Access rules are composed based on the network activity information of applications installed on this computer.

To configure mode parameters:

1. Go to the Learning mode section of the firewall configuration.



2. If it is necessary to enable learning mode, click "Permanent learning from" or "Set learning interval" and specify the start date or an interval for this mode to be active.
3. Configure the learning mode parameters.

Field	Value
Activate rules after the end of learning	Select this checkbox if you want all rules composed during the active period of the learning mode to apply upon the its completion
Direction	Specify the traffic direction to apply learning mode to
Maximum number of rules to be generated	Type the maximum number of rules to be generated while the learning mode is active
Maximum number of rules that can be generated for the application	Type the maximum number of rules to be generated while the learning mode is active for each application
Save information about the process	Select this checkbox for the generated rules to be active for particular applications whose processes caused network activity. If the checkbox is left clear, rules will be generated for all applications
Save information about remote/local host ports/addresses	Select the corresponding check boxes to save the necessary information

4. To save the new parameter values, click the Apply button in the top of the Settings tab.

   Learning mode will be configured based on the defined parameter values.

Tip. Use the By default button to restore the table's original version.

Managing the firewall on protected computers

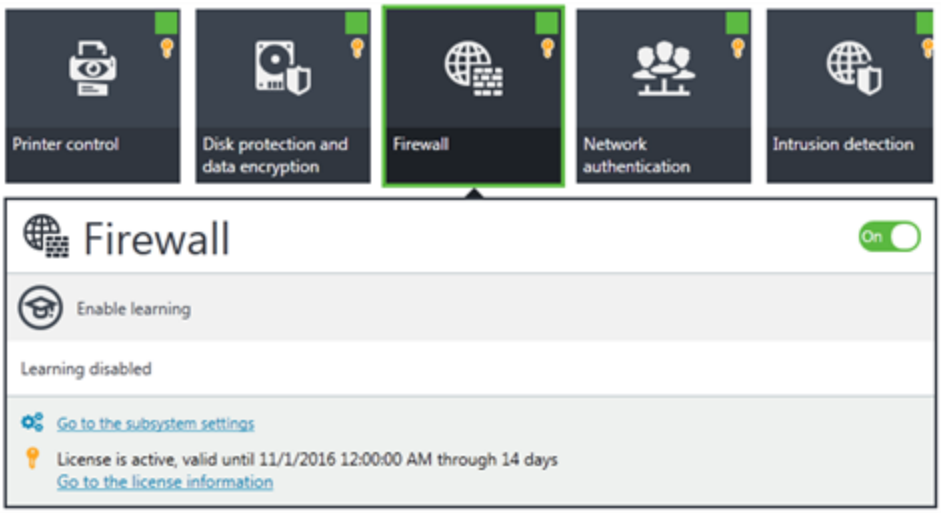
The Secret Net Studio Control Center makes it possible manage learning mode on a single computer.

To manage the firewall:

1. In the object list right-click the computer you need to configure and click Properties.

   An information window with computer status appears.
2. Open Status tab and select the Firewall element.

   The firewall control panel appeas.



3. Click the Enable learning/Disable learning button to manage the learning mode. Learning mode allows you to create a basic set of access rules (see p. **31**).

Note. Click the "Go to the subsystem settings" link to configure local firewall policies.
Click the "Go to the license information" link to see current license information.

Chapter 3
Network authorization

The network authentication mechanism is configured centrally via the Control Center. Configuration is performed at the "Computer" object level, separately for each protected computer.

Note. Secret Net Studio also includes the Local Control Center component. This component allows you only to view network authentication mechanism settings on a protected computer.

To configure these parameters:

1. Open the Control Center.

   The main program window appears.

   Tip. To view network authentication mechanism settings directly on a protected computer, open the Local Control Center, click the "Settings" tab and select the "Network authentication" element in the "Policies" section. Parameters cannot be configured in the local mode.

2. Open the "Computers" view and select the computer you need on the left side of the window. Right-click the selected computer and click "Properties".

   A list of parameters and policies for this computer appears on the right side of the window.

3. Click the "Settings" tab and select the "Network authentication" element in the "Policies" section.

   Interface for authentication mechanism configuration appears on the middle of the window.

4. Configure the required parameters and click the "Apply" button to save changes.

Configuring connection protection for the <everyone> group

To allow network connection protection in access rules configured for the <everyone> group, select the "Enable connection protection" check box.

Configuring packet processing parameters

Secret Net Studio has a networking protection mechanism for authorized subscribers. This mechanism based on the IPsec framework open standards and ensures data exchange security.

The current version uses the following protocols.

Name	Description
AH (Authentication Header) protocol	Guarantees transferred data authenticity and integrity for each IP packet. Ensures protection against the Man-in-the-middle attacks
ESP (Encapsulating Security Payload) protocol	Encodes and controls transferred data integrity
ISAKMP (Internet Security Association and Key Management Protocol)	Ensures key exchange and connection parameter regulation

There are several configuration modes. The Administrator can set an individual protection mode for each protected computer.

The network authentication default parameters are configured as follows:

- the packet signature mode with "Whole packet" signature level is enabled;
- anti-replay-attack protection mode is enabled;

- the SMB connection user defining scenario is run as a user account.

Transferred data protection and integrity is ensured through:

- packet signature mode — AH protocol in transfer mode, hashing algorithm: HMAC-MD5;
- encryption and integrity control mode — ESP protocol in transfer mode, encoding algorithm — AES CBC 128, hashing algorithm: HMAC-SHA;
- anti-replay-attack protection mode: ISAKMP.

Note. The current version of the system does not allow simultaneous use of AH and ESP protocols.

To configure these parameters:

1. In the "Network authentication" menu, select the Settings | Network packet processing section:

2. Configure the network packet protection parameters.

Attention! To establish a secure connection:

- configure access rules for a remote receiving computer required exchanging data with a sending computer (see p. 8);
- enable IP packet signature mode on the sending computer.

If any of these conditions are skipped, a secure connection cannot be established.

Parameter	Description
Signature	Select this option button to enable packet signature mode, then select a signature level: • Only marking — only the first packet in the series is signed, the rest are marked to be identified as part of an authenticated series; • Packet headers — headers of each packet are signed; • Whole packet — each packet is signed as a whole. Whether an outgoing packet is signed or not is defined by the security parameters of the remote computer (IP packet receiver). If the receiving computer allows data exchange with the sending computer and the corresponding rules are configured, all packets sent to that computer will be signed once the packet signature mode is enabled
Encryption	Select this option button to enable data encryption
Integrity Check	Select this check box to enable integrity control for encoded packets. If integrity control is not required for packets, uncheck the "Integrity Control" check box
Protection against replay attacks	Select this check box to activate the protection mode that will prevent passive data capture and transmission

Configuring an SMB connection

There are the several scenarios in Secret Net Studio for determination the user of an SMB connection:

- the computer account is always considered as an SMB connection user;

- a connection user is the account of a user who initiates it. Note that other users are either authorized or unauthorized to use an established SMB connection.

All activity of users authorized to use this connection type occurs through the account of the initiating user. If a connection-initiating user is inactive for more than 30 seconds, the next user or service in line requiring an SMB connection is considered as the actual connection user.

Priority to be provided with an SMB connection (bottom to top): anonymous users, services, authorized Secret Net Studio users.

When implementing a scenario where a connection user is a connection-initiating user, other users are:

- authorized to use the SMB connection — all low priority subscriber activity occurs through the higher priority subscriber;
- unauthorized to use an SMB connection — upon request of a higher priority subscriber to use a connection, it becomes unavailable to lower priority subscribers.

To select a scenario:

1. Select the Settings | Scenario for SMB connection user definition section.

Note. If an SMB connection is created before the mechanism component is launched (e.g., a mapped drive with the selected "reconnect at login" check box), the priority of service equals that of the users, and all further connections will occur through the computer account.

2. Specify a scenario to define an SMB connection user.

Parameter	Description
As computer account	Select this option button for SMB connections to be established under the computer account
As user account	Select this option button for SMB connections to be established under the user account
Block SMB traffic of other users	Select this check box for SMB connections to be restricted for all, except the connection initiating user

Comment. All users will be granted access to an object through a single account (the first that accesses to the terminal server) under the following condition:

- access to a protected object is granted through a terminal server;
- the SMB connection is established under a user account;
- the "Block SMB traffic of other users" check box is unselected.

If the "Block SMB traffic of other users" check box is selected, a connection will only be accessible to the user who initiated the connection to the terminal server.

If computer accounts are used, all users of the terminal server will be granted access to a protected object through the same single account.

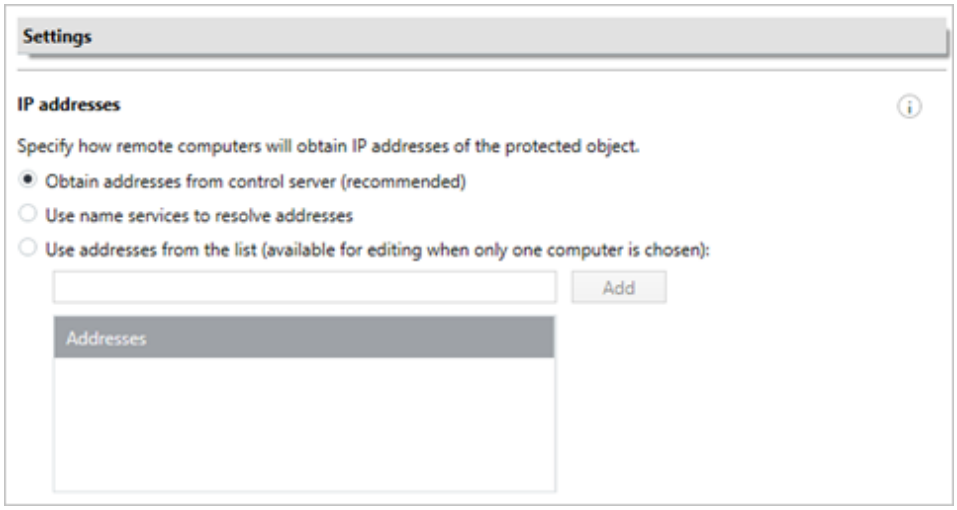
3. To save the new parameter values, click the "Apply" button in the top of the "Settings" tab.

Configuring the computer's IP address acquisition parameters

Secret Net Studio network protection tools allow a computer to be identified by both its name and its IP address. It can be used when a computer name is not automatically converted to an IP address.

To configure these parameters:

1. In the "Network authentication" menu, select the Settings | IP addresses section.



2. Configure the parameters.

Parameter	Description
Obtain addresses from control server	By default, the Clients will automatically acquire IP addresses for a protected computer from the Security Server governing this computer
Use name services to resolve addresses	Select this option button for the Clients to refer to the DNS, WINS and NetBIOS services to acquire addresses
Use addresses from the list	Select this option button if you want to explicitly specify the addresses. Type the IP address of a protected computer in the text box and click Add. To remove the entered IP address, select it from the list and click Delete

3. To save the new parameter values, click the "Apply" button in the top of the "Settings" tab.

Managing the network authorization mechanism on protected computers

The Control Center makes it possible to manage the work of the network authentication mechanism on a single selected computer.

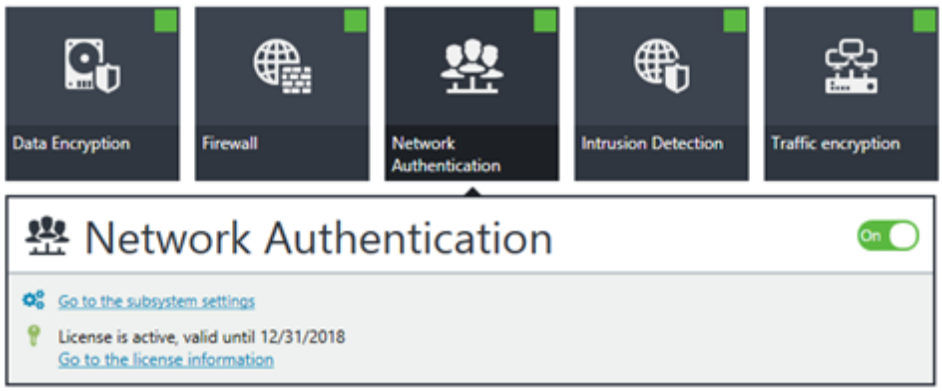
To manage the network authentication mechanism

1. Select the computer from the object list, right-click the selected computer and click Properties.

   An information about the computer status appears.

2. In the "Status" tab, select the "Network authentication" element.

   A control panel to manage the network authentication mechanism appears.



3. To enable network authentication on a protected computer, move the switch to the "On" position.

Note. Click the "Go to the subsystem settings" link to configure local firewall policies.
Click the "Go to the license information" link to see current license information.

Documentation

1.	Secret Net Studio. Administrator's manual. Development principles
2.	Secret Net Studio. Administrator's manual. Installation and update
3.	Secret Net Studio. Administrator's manual. Setup and operation
4.	Secret Net Studio. Administrator's manual. Centralized management, monitoring and audit
5.	Secret Net Studio. Administrator's manual. Setup and operation. Local protection
6.	Secret Net Studio. Administrator's manual. Setup and operation. Network protection
7.	Secret Net Studio. Administrator's manual. Setup and operation. Antivirus and intrusion detection tool
8.	Secret Net Studio. User manual