SECURITY code

Continent Enterprise Firewall
Version 4

IPS

Administrator guide

Mailing address:	**115230, Russian Federation, Moscow, 1st Nagatinsky proezd 10/1**
Phone:	**+7 (495) 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**www.securitycode.ru**

Table of contents

List of abbreviations

DNS	Domain Name System
FTP	File Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
IPS	Intrusion Prevention System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

Introduction

This manual is designed for administrators of Continent Enterprise Firewall, Version 4 (hereinafter — Continent). It contains information about the Intrusion Prevention System configuration and management.

This document contains links to documents [**1**] and [**2**].

Website. Information about SECURITY CODE LLC products can be found on https://www.securitycode.ru.

Technical support. You can contact technical support by phone: +7 800 505 30 20 or by email: support@securitycode.ru.

Training. You can learn more about hardware and software products of SECURITY CODE LLC in authorized education centers. The list of the centers and information about the learning environment can be found on https://www.securitycode.ru/company/education/training-courses/.

You can contact a company's representative for more information about trainings by email: education@securitycode.ru.

Version 4.1.9 — Released on May 22nd, 2024.

Chapter 1
How IPS works

The Intrusion Prevention System analyzes network traffic to detect cyber attacks on the network level (L3 IPS).

Continent supports two operation modes for a Security Gateway with the enabled Intrusion Prevention System:

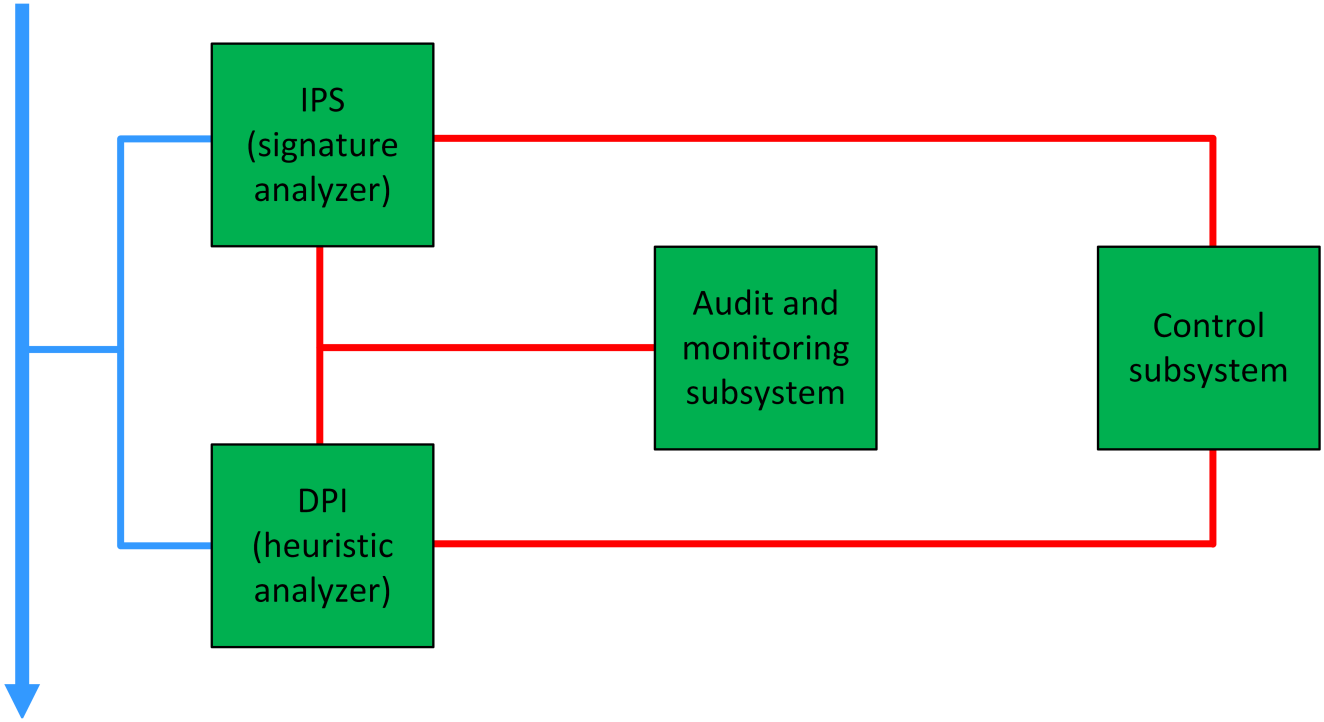
- **UTM** — packets are sent to the IPS after being processed by the Firewall. If you disable the Firewall on the Security Gateway with the enabled IPS, all traffic is automatically sent to the IPS. The IPS in **UTM** mode can be configured only in **Inline** mode (see below).
- **IPS** — the IPS does not modify packets. The Firewall is not enabled. The IPS appliance can be configured in **Monitor** and **Inline** modes.

The IPS can operate in the following modes:

- **Monitor**

  In this mode, traffic is mirrored to the IPS from a SPAN port of a switch or a router.

  If an attack is detected, the IPS appliance registers it and sends information about it to the Security Management Server.

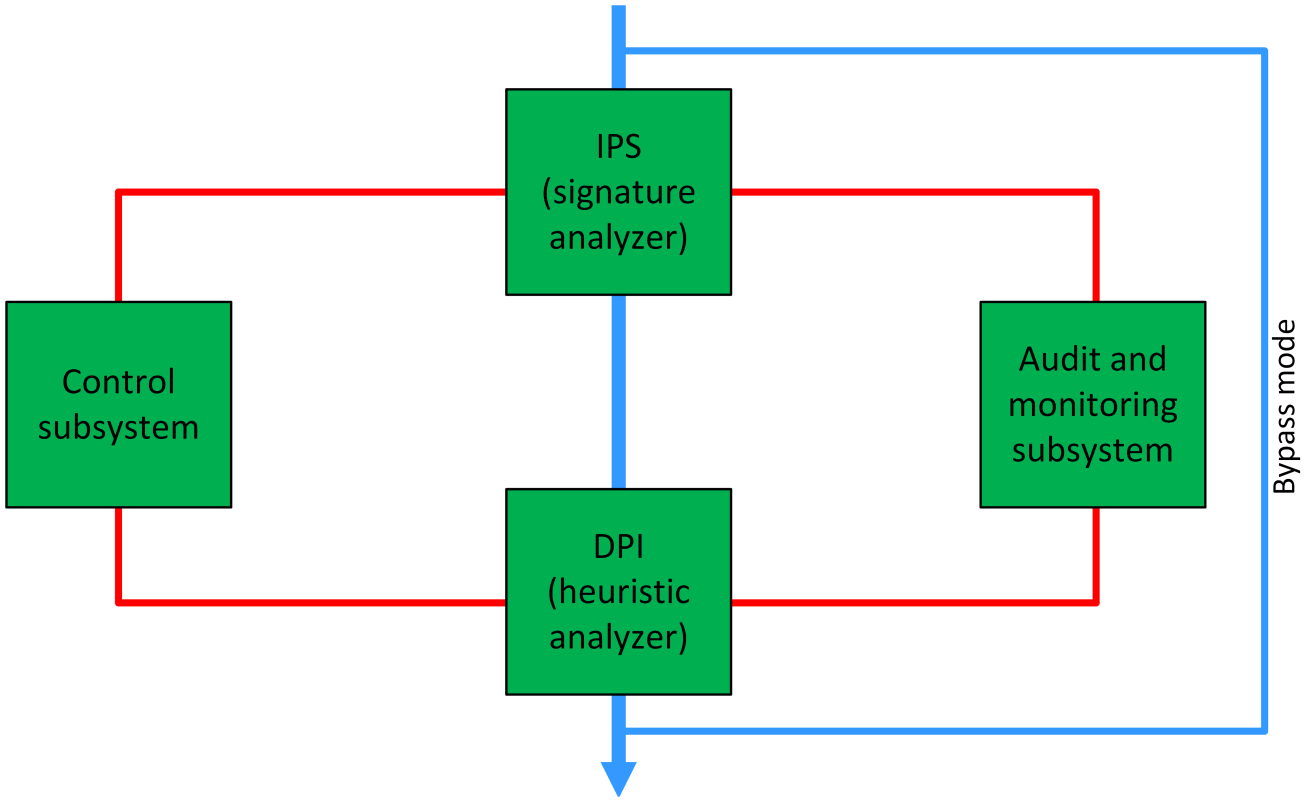


- **Inline**

  In this mode, the IPS appliance is placed between the Internet and a protected network. In case of a traffic analyzer software failure, the IPS appliance switches to bypass mode for traffic to pass (when the respective option is enabled).

  Traffic is captured and sent using physical interfaces. You can use several pairs of interfaces.

  If an attack is detected, the IPS appliance registers it and drops malicious traffic if it is prescribed in an IPS policy. The Security Management Server receives information about the attack.



The IPS analyzes data using a signature method based on IPS protections. You should upload IPS protections to the Security Management Server, then include the required ones in the IPS profile. To apply the IPS protections included in the IPS profile to the IPS appliance, an administrator must create an IPS policy rule that includes the required IPS profile, then install it on the required IPS appliance.

The IPS profile contains a custom heuristic analyzer to control application traffic.

The Security Code IPS protections set is divided into groups by default. You cannot modify a single vendor IPS protection or the whole set. The IPS administrator can create and modify custom IPS protections and groups. You may use a vendor IPS protection as a template for a custom one (see p. **18**).

Each IPS protection defines a counteraction (alert, drop or pass) to an attack signature for each IPS profile separately. The IPS administrator can modify the attack counteraction of the IPS protection or the IPS profile according to the IPS appliance operation mode. In **Monitor** mode, the IPS appliance can only notify the administrator about a detected attack. In **Inline** mode, the IPS appliance can counteract the attack in any existing way.

The syntax of an IPS protection is described in the Appendix (see p. **27**).

Chapter 2
IPS configuration

To configure the IPS:

1. Upload the IPS license to the repository.
2. Configure the Security Gateway with the enabled IPS component according to the required operation mode (see below).
3. Create a set of custom IPS protections (see p. **16**).
4. Create and configure the IPS profile (see p. **19**).
5. Create the IPS policy rules (see p. **22**).
6. Save the configuration (see p. **25**)
7. Install the policy on the Security Gateway with the enabled IPS component and the Security Management Server (see p. **25**).

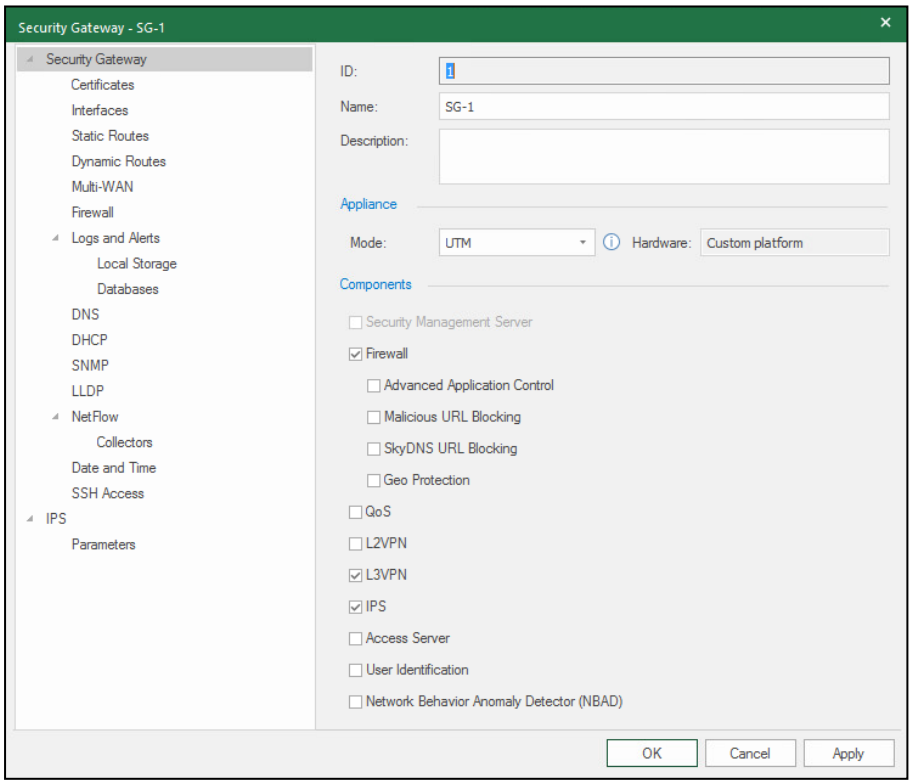
Configure the Intrusion Prevention System in UTM mode

To configure the IPS parameters:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
2. If necessary, modify the name and the description.
3. In the **Appliance** group box, select **UTM** in the **Mode** drop-down list.

   The list of available Continent components changes.
4. In the list of components, select **IPS**.

   The **IPS** menu item with the **Parameters** submenu appears on the left.



5. Click **OK**.

   The Security Gateway properties dialog box closes.

Configure the Intrusion Prevention System in IPS mode

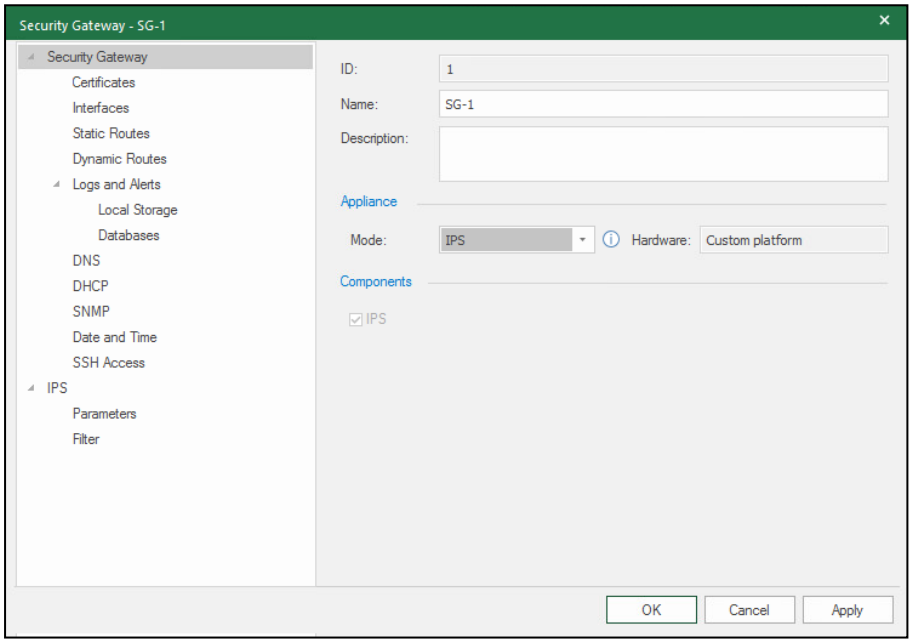
When configuring the IPS after selecting the **IPS** mode, you need to add interfaces for the selected scheme (**inline** or **monitor**) right away.

After configuring the interfaces, you need to create rules for this Security Gateway in **IPS | IPS policy** (see p. 22). Then you can apply the policy to the IPS and the Security Management Server (see p. 25).

To configure IPS parameters:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
2. If necessary, modify the name and the description.
3. In the **Appliance** group box, select **IPS** in the **Mode** drop-down list.

   On the left, the **IPS** menu item with the **Parameters** and **Filter** submenus appears. The list of available Continent components changes.



4. Click **Apply**.

   The Security Gateway dialog box closes.
5. Go to **Structure**, select the respective Security Gateway and click **Update** in the shortcut menu.

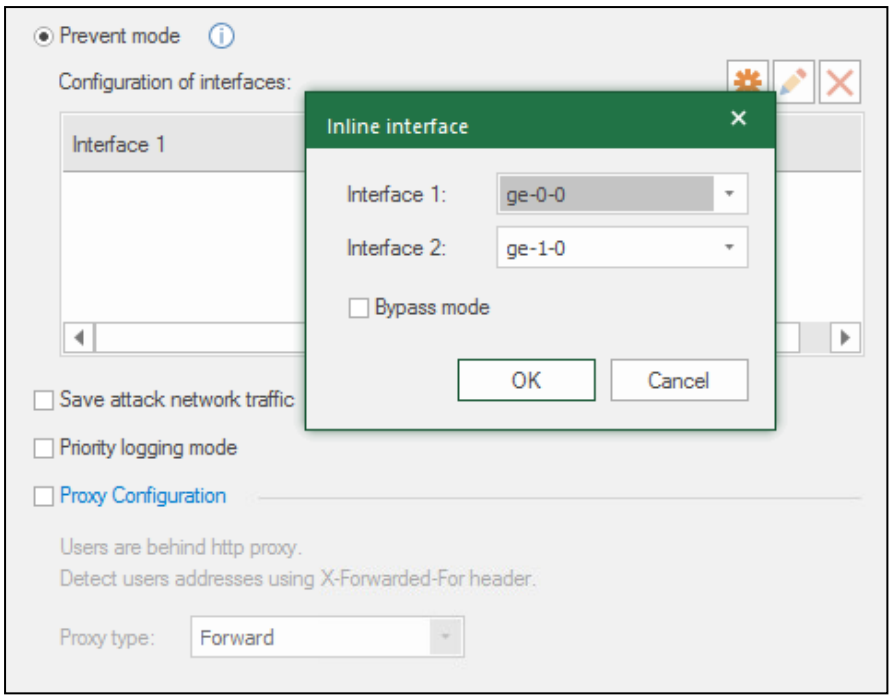
Configuring the IPS appliance in Inline mode

To configure parameters:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway with the enabled IPS component and click **Properties** on the toolbar.
2. Go to the **IPS** section.

   The settings of the IPS appliance operation mode appear.
3. Select the **Inline mode** check box and click to add the Inline interfaces to the commutation list.

   The **Inline interface** dialog box appears.



4. Select the required logical interfaces for each physical Inline interface.
5. If necessary, select **Bypass mode** to pass traffic in case of an IPS appliance failure, then click **OK**.

   Note.
   When bypass mode is enabled, an additional interface is created to redirect traffic bypassing the IPS. With overloaded traffic, IPS may fail. In this case, traffic is redirected to the created bypass interface. After the IPS is restored, bypass mode is disabled and traffic passes through the IPS.

   The notification about the assigned Inline interfaces appears.
6. Click **Yes**.

   The assigned interfaces appear in the list.
7. If necessary, select **Save attack network traffic**.

   In this case, the corresponding file in PCAP format will be available for downloading in the security log with the detailed information about the event.
8. If necessary, select the **Priority Logging Mode**.

   This mode is enforced by the requirements of a security policy if it is necessary to record all attacks. In this case, performance degradation of the IPS can take place.
9. Click **OK**.

   All changes are saved and the Security Gateway dialog box closes.
10. To apply changes, click **Install policy** on the toolbar, select the required Security Gateway and click **OK**.

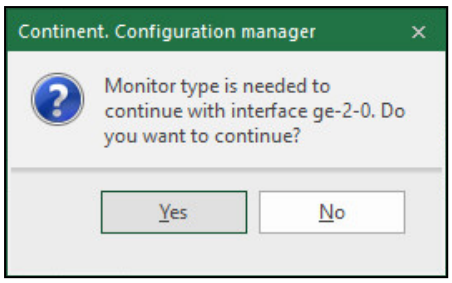
Configuring the IPS appliance in Monitor mode

To configure parameters:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway with the enabled IPS component and click **Properties** on the toolbar.

   The Security Gateway properties dialog box appears.
2. On the left, select **IPS** and select the **Monitor mode** option button.

   The **Commutation** list becomes available for editing.
3. If the monitoring interface is not specified, click  and select the required physical interface. Click **Yes**.



4. If necessary, select **Save attack network traffic**.

   In this case, the corresponding file in PCAP format will be available for downloading in the security log with the detailed information about the event.

5. If necessary, select **Priority Logging Mode**.

   This mode is enforced by the requirements of a security policy if it is necessary to record all attacks. In this case, performance degradation of the IPS can take place.

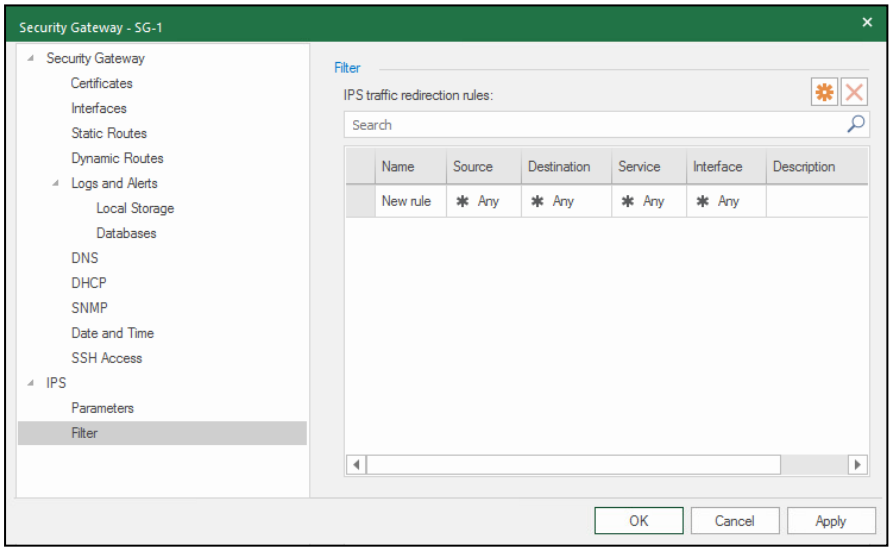
6. On the left, go to **IPS | Filter**.

   Rules in **Filter** pass traffic to IPS in order to process it. On the right, you can see the filter rules created for the IPS.

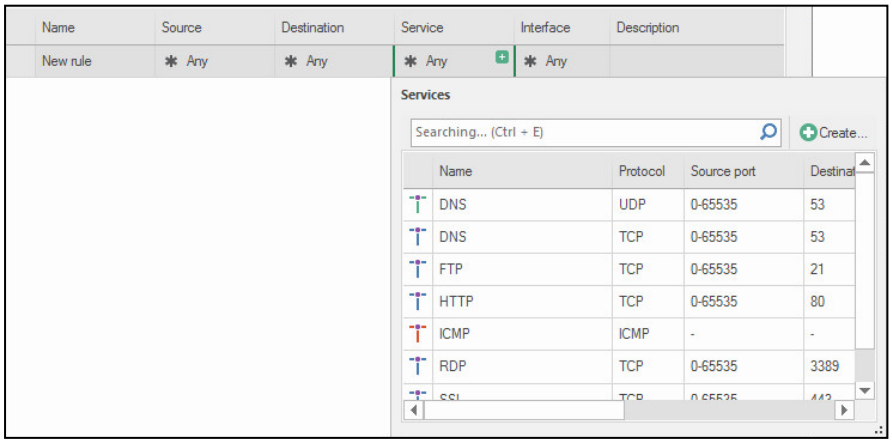
   Note.
   If no rules were created, the list is empty.

7. To add a new rule, click .

   The created rule is added to the list.



8. Set the required parameters in the respective columns using double-click, , or .



9. If necessary, add more rules to the list.
10. Click **OK**.

    All the changes are saved and the Security Gateway dialog box closes.

IPS parameters

To configure IPS parameters:

1. Go to **IPS | Parameters**.

> **Note.**
> The IPS parameters are used to define home and external networks. They are used in vendor and custom IPS protections to set a source and a destination.

A list of parameters appears as in the figure below.

Name	Network objects / Service	Inversion
AIM_SERVERS	$HOME_NET	☐
DNP3_CLIENT	$HOME_NET	☐
DNP3_PORTS	20000	☐
DNP3_SERVER	$HOME_NET	☐
DNS_SERVERS	$HOME_NET	☐
ENIP_CLIENT	$HOME_NET	☐
ENIP_SERVER	$HOME_NET	☐
EXTERNAL_NET	!$HOME_NET	☐
HOME_NET	[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]	☐
HTTP_PORTS	[80,81,311,591,593,901,1220,1414,1830,2301...	☐
HTTP_SERVERS	$HOME_NET	☐
MODBUS_CLIENT	$HOME_NET	☐
MODBUS_SERVER	$HOME_NET	☐
ORACLE_PORTS	1521	☐

2. To configure the parameters, double-click the **Network objects / Service** cell of the required parameters and specify the respective information.

> **Note.**
> To search for parameters, use the respective search text box at the top of the **Security Gateway** dialog box.

To specify network objects or services, use a comma (**,**) between them (the contents must be taken into brackets), other parameters (in the **$Parameter_name** format) and the inversion (or use **!** before the parameter name). You can create a new IPS parameter by clicking  .

> **Note.**
> It is required to use the specified data format to configure IPS parameters. If invalid IPS parameters are set, a policy is applied successfully but the IPS stops functioning. The error message appears in the system log (for example, in the HOME_NET parameter). To view error details, go to the System log and reset the filter. Then, filter data by importance **ERR** and by **System** category.

> **Note.**
> You can set an inversion of custom IPS parameters via the parameter context menu. For setting an inversion of built-in IPS parameters, enter **!** before the parameter.

3. Click **Apply**.

Configure a proxy server

To configure a proxy server:

Note.
When using a proxy server, the IPS can use the built-in tools to identify the sender behind the proxy or proxy chain. The forward and reverse proxy methods are different.

1. In the Configuration Manager, go to **Structure**.
   The list of the Security Gateways appears in the display area.
2. Select the Security Gateway with the enabled IPS component and click **Properties** on the toolbar.
   The properties of the selected IPS appliance appear.
3. On the left, go to the **IPS** section and select the **Proxy Configuration** check box.
4. In the **Proxy type** drop-down list, select the required option (**Forward** or **Reversed**) and click **OK**.
5. To apply changes, click **Install policy** on the toolbar, select the required Security Gateways and click **OK**.

Management of IPS configuration

Manage IPS protections

Updating IPS protections

The IPS protections are downloaded and updated automatically or manually to the Security Management Server database. To apply the updated IPS protections to the Security Gateways, change the respective IPS profiles (see p. 19).

If IPS protections are updated after an update license has expired, the policy installation will lead to the following:

- new rules are not installed on the IPS appliance;
- rules deleted from the updated IPS protections list are also deleted from the IPS appliance;
- rules modified in the updated IPS protections list remain unmodified on the IPS appliance.

Examples:
When you update IPS protections before the update license has expired:
- The IPS appliance has IPS protections installed.
- The IPS protections are installed on the Security Management Server database.
- The update license expires.
- The policy with the updated IPS protections is installed on the IPS appliance.

Result: IPS protections not contained in the updated IPS protections list are deleted, new IPS protections are installed, modified IPS protections are updated.

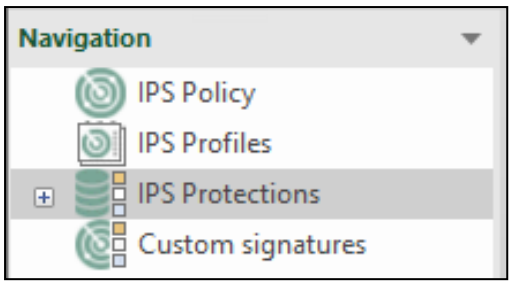
When you update IPS protections after the update license has expired:

1. The IPS appliance has IPS protections installed.
2. The update license expires.
3. The IPS protections are installed on the Security Management Server database.
4. The policy with the updated IPS protections is installed on the IPS appliance.

Result: IPS protections not contained in the updated IPS protections list are deleted, new IPS protections are not installed, modified IPS protections are not updated.

To update IPS protections locally:

1. Prepare the update file received from the vendor.
2. In the Configuration Manager, go to **IPS** and select **IPS protections**.



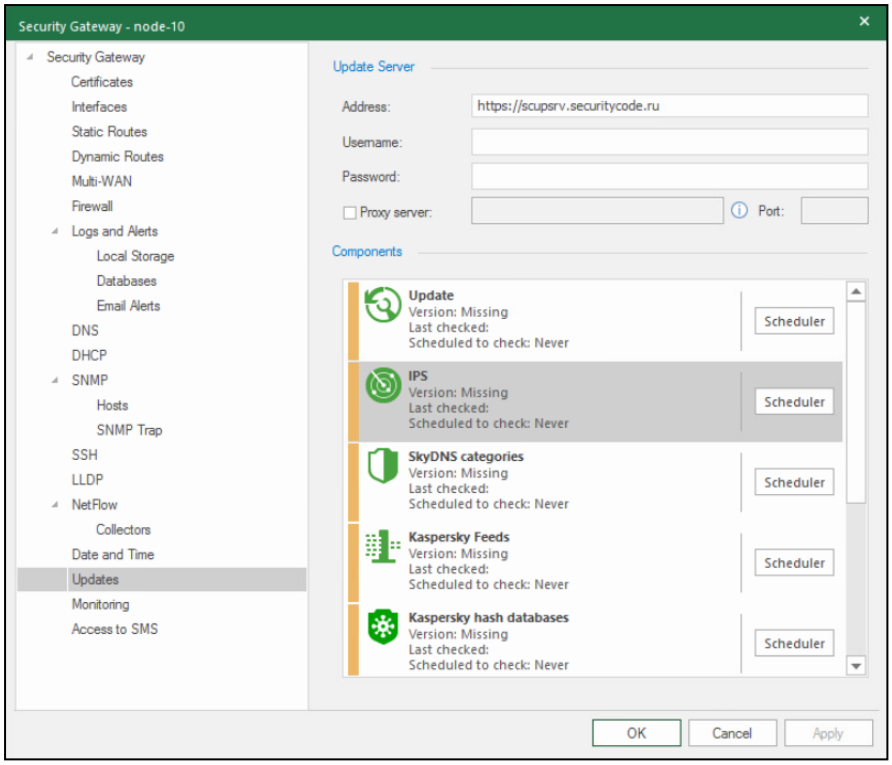
3. On the toolbar, click **Import**.
   The File Explorer dialog box appears.
4. Select the required update file and click **Open**.
   When the IPS protections are uploaded, you receive the respective message.
5. Click **OK**.
   The list of the updated IPS protections appears in the display area.

IPS protection						IPS profile		
Severity	Description	Class	Revisi...	SID		Full set	Optimal set	Recommended set
High	SSL Cert Used In Unknown Exploit Kit	Potentially malicious ssl-cer...	1	4115...		Drop	Inactive	Inactive
High	Possible Locky AlphaNum Download...	Trojan	2	4123...		Drop	Drop	Drop
Middle	Known Tor Relay/Router (Not Exit) N...	Potentially malicious traffic	3281	4213...		Alert	Inactive	Inactive
High	W32/Liftoh.Downloader Get Final Pa...	Trojan	3	4117...		Drop	Drop	Drop
High	Win32/CryPy Ransomware Encryptin...	Ransomware	2	4123...		Drop	Drop	Drop
Middle	portmap SET attempt TCP 111	Potentially malicious traffic	6	4201...		Alert	Inactive	Inactive

6. Save changes in the domain configuration by clicking in the top left corner of the Configuration Manager. Install the policy on the required Security Gateway (see p. **13**).

To update IPS protections on schedule using the Update server:

1. In the Configuration Manager, go to **Structure**.
2. Select the Security Management Server and click **Properties** on the toolbar.
   The **Security Gateway** dialog box appears.
3. On the left, select **Updates**.
   Parameters for automatic software update appear.



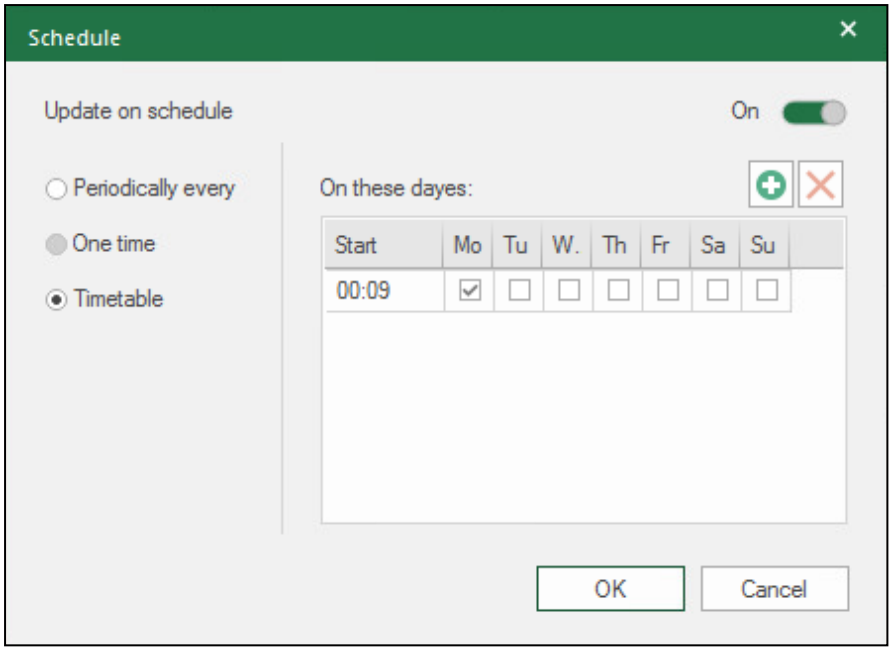
4. Check the Update server address in the respective field.

> **Attention!**
> The HTTPS protocol is required.

5. Specify the administrator's credentials.

> **Note.**
> To obtain the credentials, contact our technical support by email at **support@securitycode.ru**.

6. If the proxy server is required, select the **Proxy server** check box and specify the respective connection parameters.
7. In the required component filed, click **Scheduler**.
8. Turn on the **Update on schedule** toggle.
9. Select the update frequency and specify the required parameters:
   - for **Periodically every** option, specify the date and time of updates and interval between them;
   - for **One time** option, specify the date and time of an update;
   - for **Timetable** option, specify the update time and days of the week.



10. Click **OK** to apply the changes.

11. Click **OK**, then click to save the configuration.

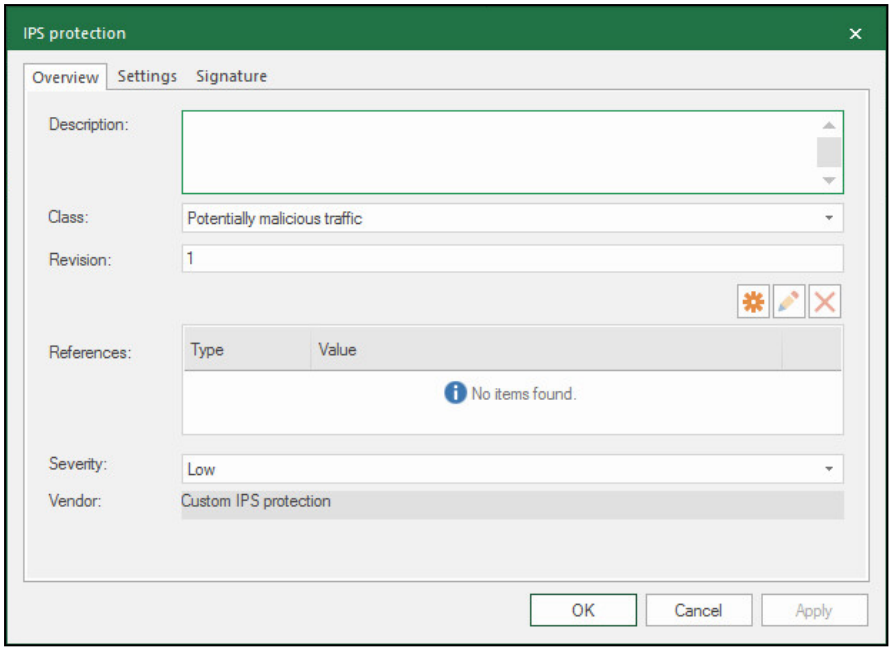
12. Install the policy on the required Security Gateways.

Creating custom IPS protections

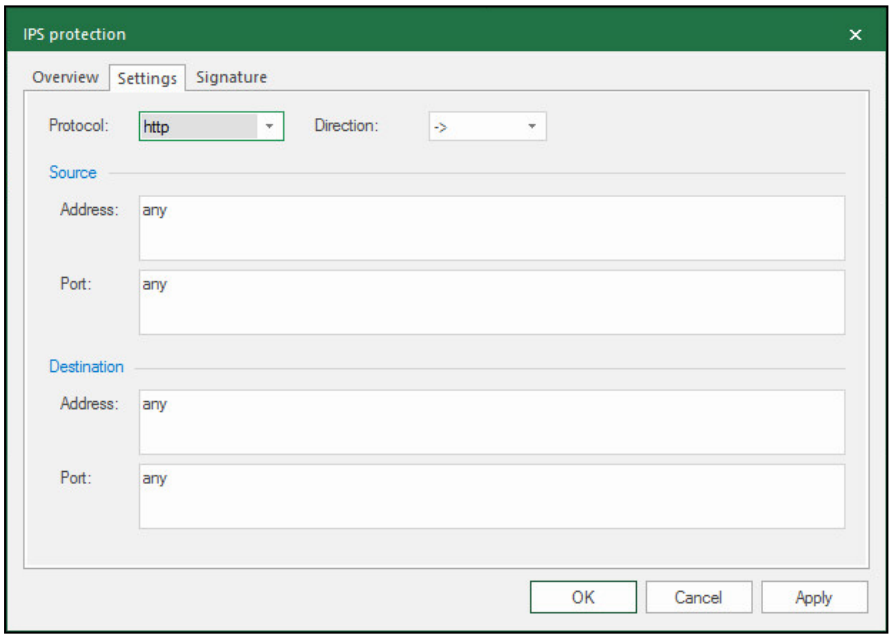
To create a custom IPS protection:

1. In the Configuration Manager, go to **IPS**, select **IPS protections**, then select **Custom IPS Protections** and click **IPS protection** on the toolbar.

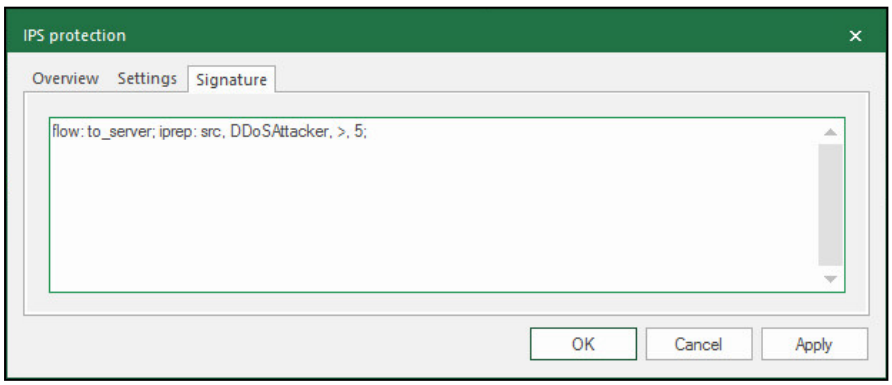
The **IPS protection** dialog box appears.



2. On the **Overview** tab, specify all the required parameters and go to the **Settings** tab.



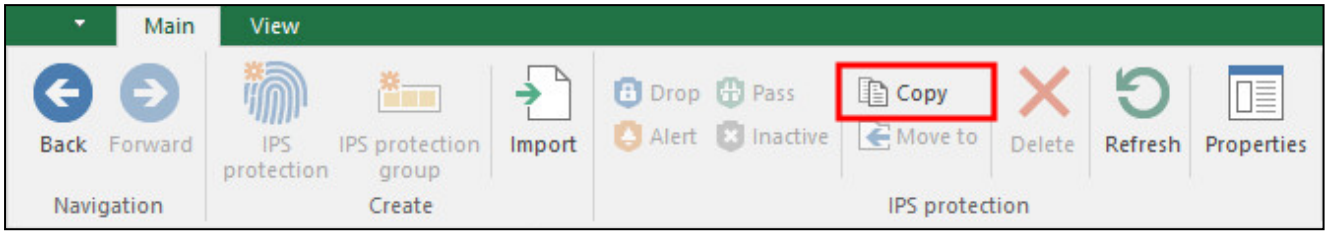
3. Specify the required IPS protection header fields (see p. **28**) and go to the **Signature** tab.



4. Specify the IPS protection options (see p. **29**) and click **OK**.
The dialog box closes and the new IPS protection appears in the list.

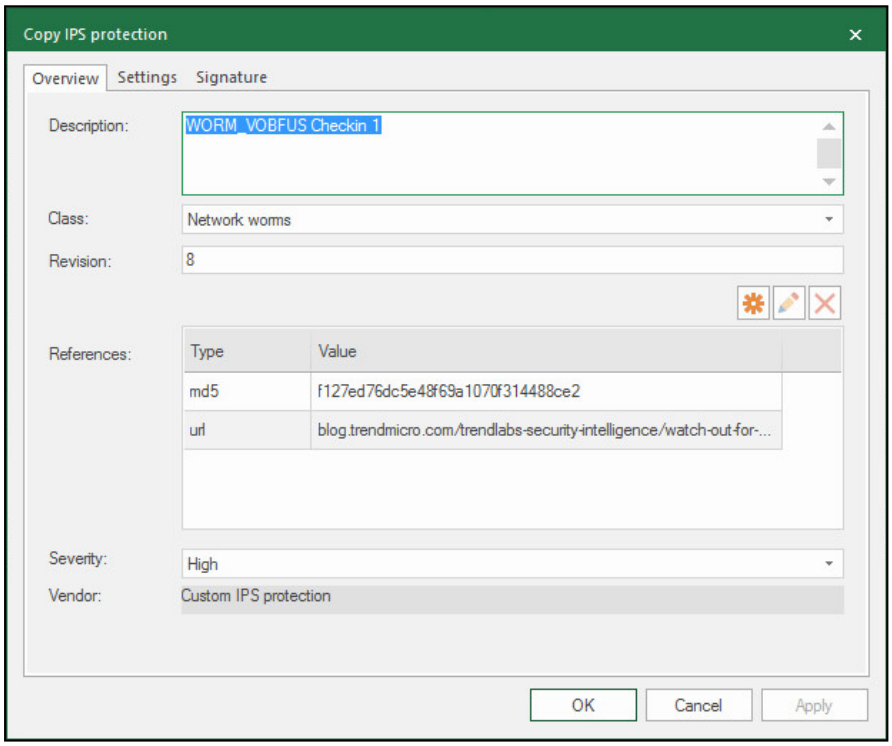
To create a custom IPS protection based on a vendor IPS protection:

1. In the Configuration Manager, go to **IPS** | **IPS Protections**, select **Security Code IPS protection**, then select the required IPS protection and click **Copy** on the toolbar.



A new custom IPS protection is created with the same parameters as the vendor one. The created IPS protection is available for editing.

The **Copy IPS protection** dialog box with the respective parameters appears.



2. Modify the content of the **Overview**, **Settings** and **Signature** tabs (see p. **27**) and click **OK**.

   The **Copy IPS protection** dialog box closes. The list of custom IPS protections with the new rule appears.

Exceptions for an IPS protection

With Continent, you can create exceptions for an individual IPS protection based on the following:

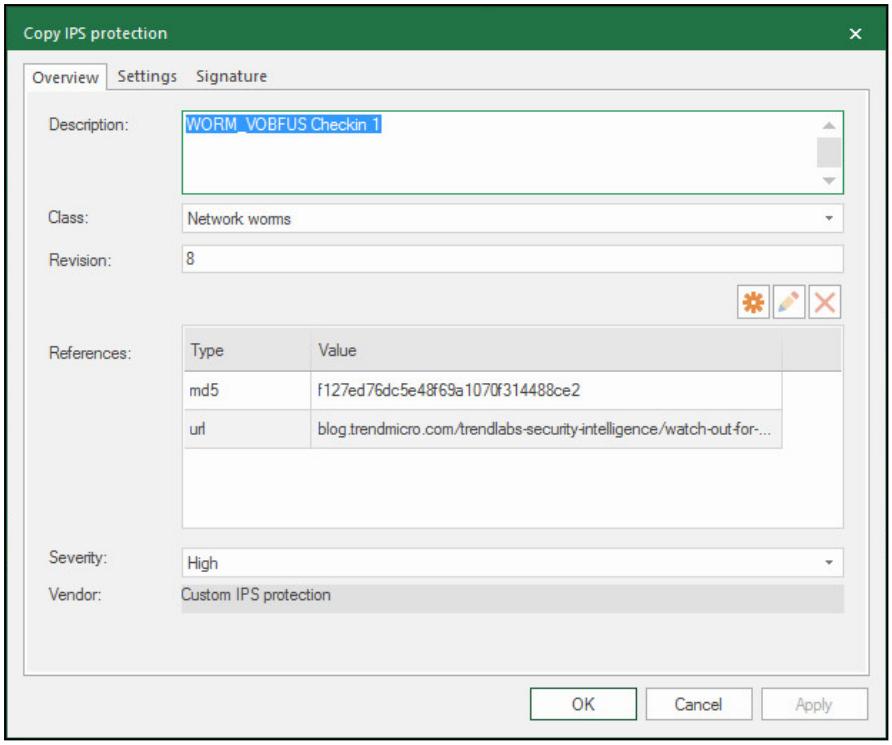
- source port;
- destination port;
- IP address, a range of destination IP addresses;
- IP address, a range of source IP addresses.

To create an exception for an IPS protection:

1. In the Configuration Manager, go to **IPS** | **IPS Protections** | **Security Code IPS Protections**.
2. Select an IPS protection and click **Copy** on the toolbar.

   A new custom IPS protection is created with the same parameters as the original one. The created IPS protection is available for editing.

   The **Copy IPS protection** dialog box with the respective parameters appears.



3. Edit parameters on the **Overview**, **Settings** and **Signature** tabs (seep. 27).

   To specify parameters, you can use conditions, for example:

```
1.1.1.1 — use a certain IP address;
!1.1.1.1 — use a whole range of IP addresses except the specified one;
[1.1.1.1, 1.1.1.2] — use the syntax in brackets as a single unit;
![1.1.1.1., 1.1.1.2] — use a whole range of IP addresses except the ones in
brackets;
[10.0.0.0/24, !10.0.0.5] — a complex condition.
```

4. Click **OK**.

   The **Copy IPS protection** dialog box closes. You are returned to the **Custom IPS protections** section. The new IPS protection exception appears in the list.

Create and configure an IPS profile

The following preset profiles are available:

- **Full set** containing a complete selection of IPS protections;
- **Optimal set** containing a basic selection of IPS protections that detect threats for data transferring services, web-clients and web-servers;
- **Recommended set** containing a selection of IPS protections that react to the most severe threats.

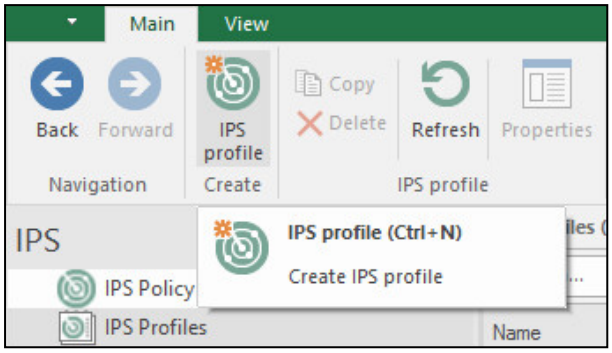
You can use these profiles to configure the IPS operation but cannot modify them.

Note.
Before creating an IPS profile, update the IPS protections (see p. 13). To do so, you need the respective license.

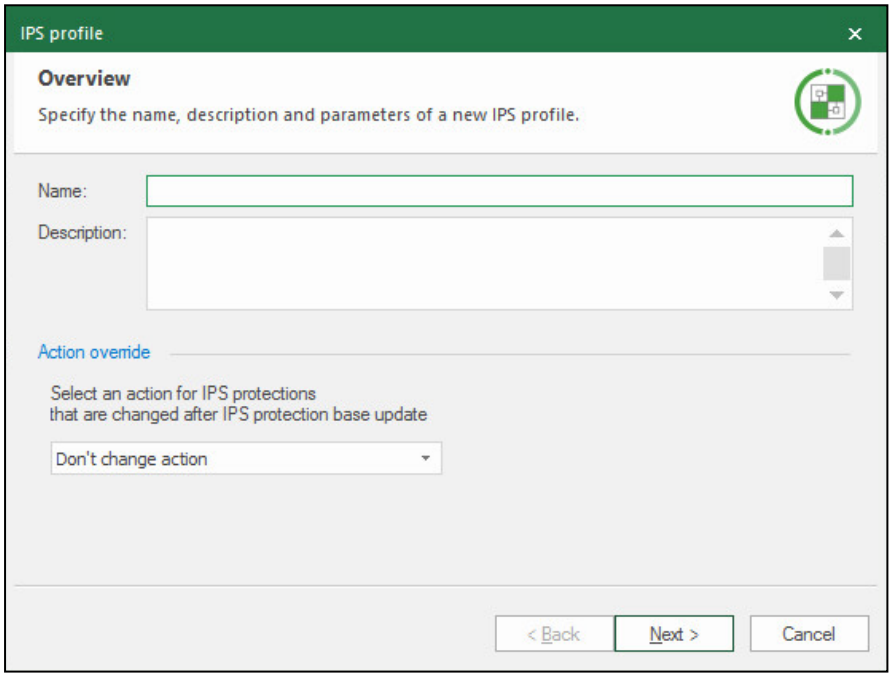
To create and configure the IPS profile:

1. In the Configuration Manager, go to **IPS**.

2. Select **IPS Profiles**.
   The list of the created IPS profiles appears in the display area.
3. On the toolbar, click **IPS profile**.



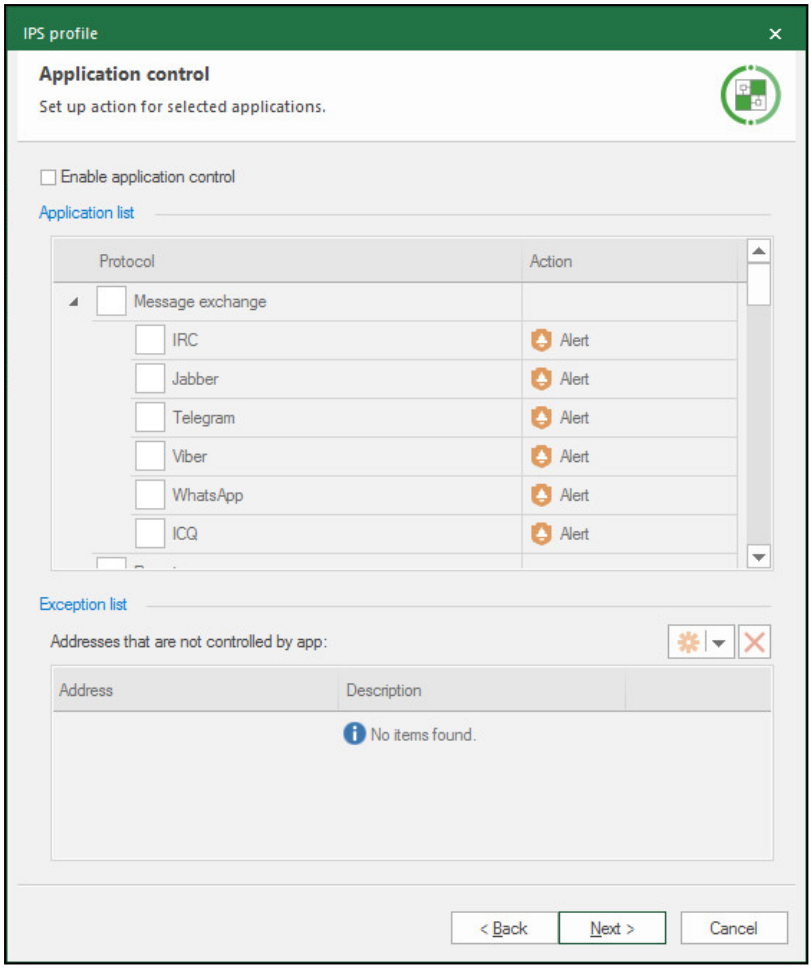
The **IPS profile** dialog box appears as in the figure below.



4. Specify the name and the description in the respective fields, select the counteraction of the IPS protections used in the profile if they have been changed after IPS protections update. Click **Next**.

Action	Description of changes in the IPS profile after the update
Don't change action	The action will not be changed for updated vendor signatures
Drop	The action will be changed to **Drop** for updated vendor signatures
Alert	The action will be changed to **Alert** for updated vendor signatures
Pass	The action will be changed to **Pass** for updated vendor signatures

The **IPS profile** dialog box appears as in the figure below.

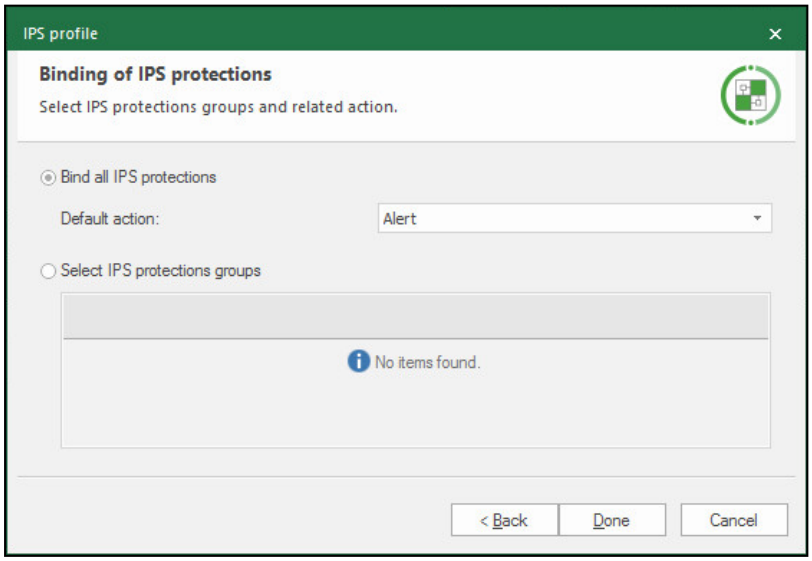


5. If necessary, select **Enable application control** and select an action for each application in the respective column.

Note.
The **Alert** action is default for every application.

6. If necessary, click  to add exceptions of network objects to exclude them from application control (to add IP address group, click **Network object** in the drop-down list) and specify the IP address and description if necessary.
7. Click **Next**.

   The **IPS profile** dialog box appears as in the figure below.



8. Select the binding type (for all the IPS protections or for individual IPS protection groups) and the default action in the respective drop-down list. Click **Done**.

Attention!
For the IPS appliances operating in the **Monitor** mode, **Drop** operates as **Alert**.

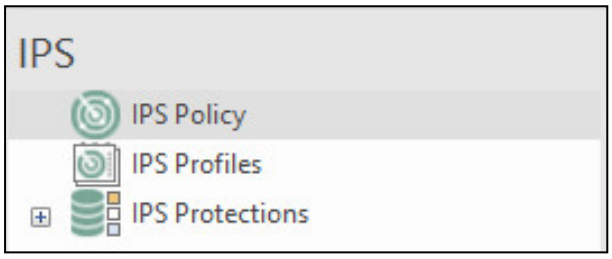
The created profile appears in the list. A column with the new profile name appears in the list of the **IPS protections**.

Note.
If the new profile column does not appear, click **Refresh** on the toolbar.

Create and configure IPS policy rules

To create and configure rules:

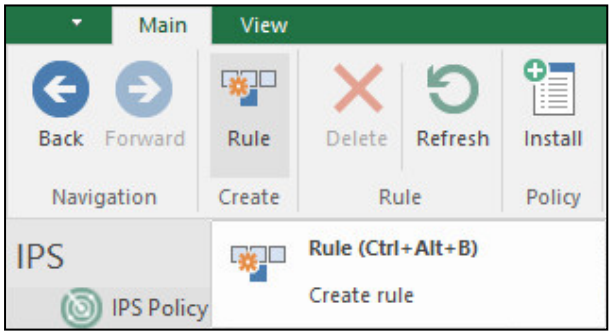
1. In the Configuration Manager, go to **IPS | IPS Policy**.



The list of rules appears in the display area.

Note.
If no rules were created, the list is empty.

2. Add a new rule by clicking **Rule** on the toolbar.



The created rule appears in the list.

3. Configure the rule parameters. Specify the required information:

Parameter	Description
Name	Enter the rule name
IPS profile	Select the required IPS profile from the list
Install On	Select the required IPS appliance to install the rule on. To delete the IPS appliance that is already specified, select it and press **<Delete>**
Description	Enter the description or comment for the rule

Manage custom signatures

View custom signature list

To view the custom signature list:

- In the Configuration Manager, go to **IPS | Custom signatures**.
  The list of custom signatures appears in the display area.

Import of custom signatures

Note.
The imported signature syntax must coincide with the following pattern:

```
action protocol source_address source_port -> destination_ address destination_port
(msg; sid; rev;)
```

The **msg** and **sid** fields are obligatory. The **sid** value cannot exceed **4,000,000**. After import, an internal Continent identifier will be assigned as the **sid** parameter.

To import custom signatures:

1. In the **Custom signatures**, click **Import** on the toolbar.
   The File Explorer dialog box appears.
2. Specify the path to the imported signature file and click **Open**.

   Note.
   Within one import procedure, you cannot download more than **50,000** custom signatures.

   After the file was downloaded successfully, you receive the respective message. If one or more signatures are not in the correct format, you receive the respective message.
3. Click **OK**.
   The downloaded custom signatures appear in the list. If the selected signature passes the check, it is assigned the **Valid** status. Otherwise, it is assigned the **Error** status.

View custom signature details

To view information about custom signatures:

1. In **Custom signatures**, select the required signature.
   In the bottom display area, detailed information about the selected signature appears.
2. If the selected signature has the **Error** status, select the **Errors** tab in the bottom display area.
   The detailed information about errors appears in the bottom display area.

Move custom signatures

To move custom signatures:

- Select the required custom signatures in the list and click **Move** on the toolbar.

  Note.
  Use **<Ctrl>** for multiple choice.

  The selected signatures will be moved to **Custom IPS Protections**.

Remove custom signatures

To remove custom signatures:

1. Select the required custom signatures, click **Remove** on the toolbar.
   The dialog box prompting you to confirm the action appears.
2. Click **Yes**.

   Note.
   Use <**Ctrl**> for multiple choice.

   The selected custom signatures will be removed.

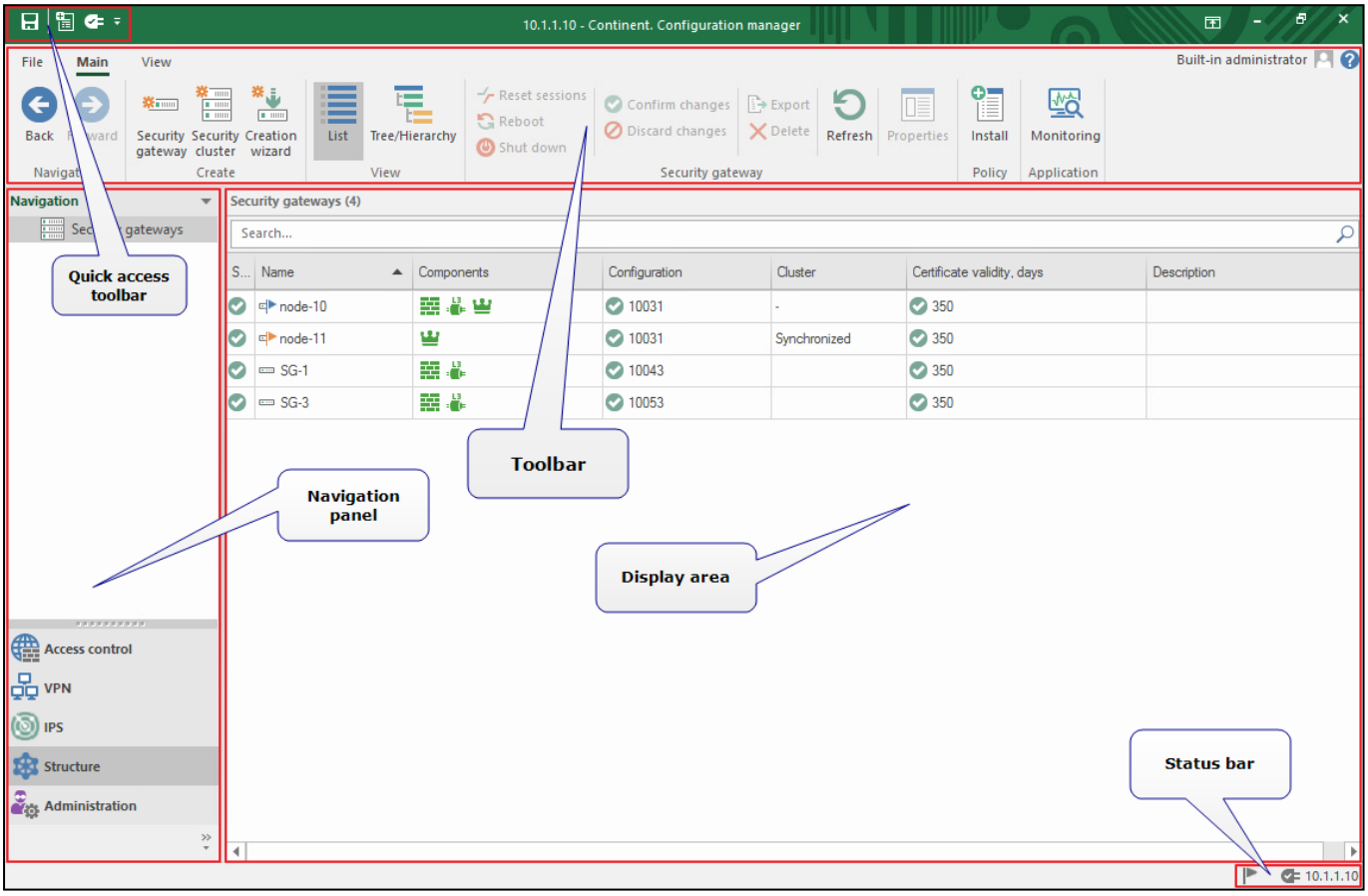
Appendix

Run the Configuration Manager

To run the Configuration Manager:

- In the Start menu, select the **Security Code** group, then click **Configuration Manager** or double-click the **Configuration Manager** icon on the desktop.

After you run and log on to the Configuration Manager, the main window appears.



The Configuration Manager window contains the following elements:

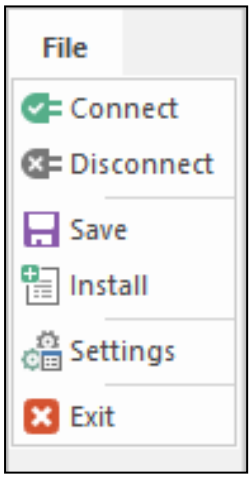
Element of the interface	Description
Toolbar	Contains a set of tools and two tabs: • **Main** — displays the toolbar; • **View** — allows configuring the interface of the Configuration Manager. Tools are buttons that you can use to launch frequently used commands. A set of tools depends on a menu item which you can select on the navigation panel. Operating conditions determine which buttons are displayed and available. When you move the pointer over a button, a tooltip appears
Quick access toolbar	Allows quick access to the most frequently used buttons. Contains the following: • — save the current configuration; • — install a security policy; • — configure the Security Management Server connections; • — connect to the Security Management Server; • — configure Quick access toolbar; • — open Quick access toolbar

Element of the interface	Description
Navigation panel	Contains the following menu items: • **Access control** — to manage Firewall and NAT rules; • **VPN** — to create and configure VPN; • **IPS** — to configure IPS settings; • **Structure** — to manage Security Gateway settings; • **Administration** — to manage service functions (operations with certificates, backups, updates, licenses, etc.)
Display area	Displays information depending on the selected navigation panel menu item
Status bar	Contains the following: • the number of tasks currently being executed and the button to open the notification center where you can find the link to open the general task list; • an icon that indicates the status of the connection to the Security Management Server (if there is a connection, this icon also displays a Security Management Server IP address, for example 10.1.1.10)
Authorized administrator	Displays information about the administrator account
About Configuration Manager	Displays information about the program, its version and copyright

Save changes in the Security Management Server configuration

To save changes in the Security Management Server configuration:

- In the top left corner of the Configuration Manager, click , then click **Save**.



Note.
You can also save changes as follows:
- press **<Ctrl>+<S>**;
- on the toolbar, click .

Install a policy

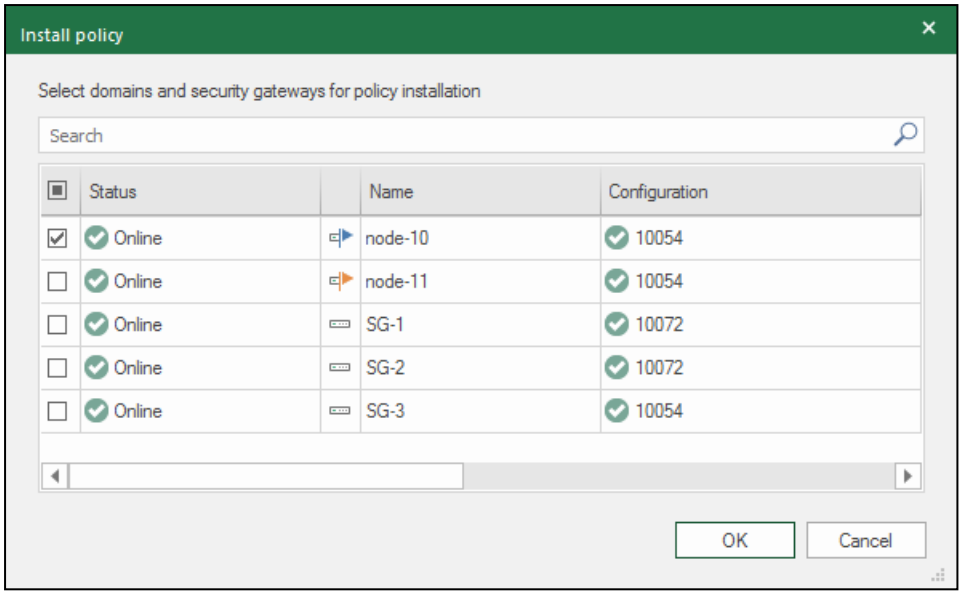
To apply changes to the Security Gateway configuration, install a policy on the Security Gateway. To install the policy, a task is created (see p. **26**). The progress of the task is displayed in the **Notification center**. The more changes to be applied, the more time is required to perform the task.

To install a policy:

1. Press **<Ctrl>+<I>**.

Note.
You can also open the **Install policy** dialog box in the **Access control**, **VPN** and **Structure** sections. To do so, click **Install** on the toolbar.

The **Install policy** dialog box appears.



2. Select the required Security Gateway and click **OK**.

   The policy installation task is created. The system starts to perform the new task if no other tasks are being performed. A number of current tasks in the queue is indicated by a numeral next to .

3. For detailed information about current tasks, click .

   The list is sorted by the time the tasks are added. When the task is performed, the respective icon appears. Then, the task is removed from the **Notification center**.

Task list

When installing a policy on a Security Gateway, the respective task is created. If no other task is currently being performed, the Security Management Server starts performing the created one. If another task is performed, the new one is registered in the system and gets in line.

Information about all created tasks is stored in the Security Management Server as a list that displays the following data:

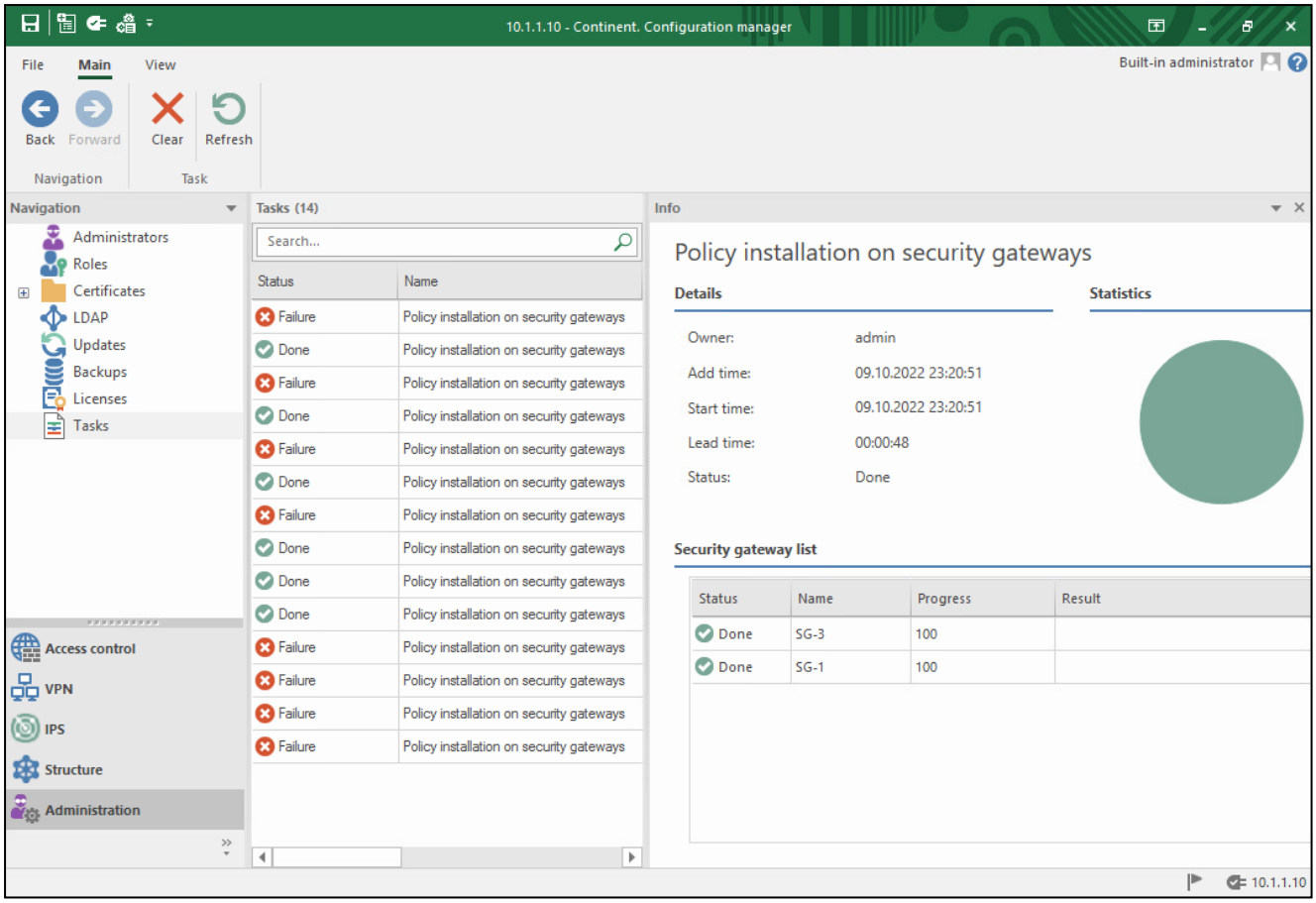
- **Name** — name of the task;
- **Owner** — name of the administrator who initialized the task;
- **Status** — status of the task;
- **Progress** — percentage completed;
- **Added** — time when the task was added to the list;
- **Started** — time when the task started;
- **Executing** — how long the task has been running.

To view the task list:

1. In the Configuration Manager, go to **Administration** | **Tasks**.

   On the right, the task list appears.

> **Note.**
>
> You can move to the task list from any section by clicking in the bottom right corner and the **Move to task list** link in the appeared **Notification center** dialog box.



The following icons are used in the task list to display the task status:

Icon	Status	Description
	Signed in	In line
	Executing	Executing now
	Done	Completed successfully
	Done with warnings	Completed but warnings are detected
	Failure	Completed with errors

2. If a task is related to applying a policy to several Security Gateways, select it in the list.

   In the additional **Info** section on the right, the detailed information about task execution on each Security Gateway is displayed.
3. To clear the task list, click **Clear** on the toolbar.

   Attention!
   This operation is irreversible.

   All tasks will be deleted from the list except for those with **Executing** or **Signed in** status.

IPS protections

IPS protection syntax

An IPS protection has the following structure:

```
<header> (<options>)
```

Options are in round brackets. Options are divided by a semicolon (**;**). Option keywords are separated from arguments by a colon (**:**).

You can write IPS protections in several strings if all the strings except the last one end with a backslash (****).

A simple IPS protection example:

```
alert tcp any any -> 192.168.1.0/24 111\
(content:"|00 01 86 a5|"; msg:"mountd access";)
```

IPS protection header

An IPS protection header has the following structure:

```
<action> <protocol> <source> <port> <direction> <destination> <port>
```

Action

The first part of the IPS protection is action reacting to signature match.

Action	Description
alert	Notifies (alert) and logs packet information to the file
drop	Drops the packet (packet is not passed). Notifies (alert) and logs packet information to the file. It can be applied only in Inline mode **Attention!** Packet dropping leads to timeout in case of using TCP.
pass	Stops scanning the packet and places it to the end of IPS protection list (only for the current packet)

The IPS protections are loaded in order of appearance in files, but processed in another order. IPS protections have different priority levels. The most important are scanned first. By default, they are organized in the following order: pass, drop, alert. You can change the priority (see **classtype** and **priority** options).

Protocol

The next header field has the protocol specified: **UDP**, **TCP**, **IP** or **ICMP**.

Source and destination

An IP address (either IPv4 or IPv6) and a subnet mask or the **any** keyword (that all the IP addresses comply with) are specified in the **Source** and **Destination** fields of the IPS protection. The mechanism correlating domain names with IP addresses is not supported, therefore specify IP addresses or CIDR blocks [RFC1518]. CIDR Block contains a network prefix and size of the mask that the IPS protection applies to all IP addresses of packets in order to check whether it matches the prefix. Block CIDR /24 means network class C, /16 — B, /32 — the exact IP address. The example of the IPS protection that reacts to packets from any address to the **class C 192.168.1.0** network:

```
alert tcp any any -> 192.168.1.0/24 111\
(content:"|00 01 86 a5|"; msg:"mountd access";)
```

You can apply the inversion symbol **!** to addresses and blocks. When using this symbol, packets not included to the specified address range comply with the IPS protection. The example of the IPS protection that reacts to packets from any address to the **class C 192.168.1.0** network (not **192.168.1.0/24**):

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111\
(content:"|00 01 86 a5|"; msg:"mountd access";)
```

You can specify addresses divided by a comma by listing them in square brackets:

```
alert tcp ![192.168.1.0/24,10.1.1.0/24] any -> [192.168.1.0/24,10.1.1.0/24] 111\
(msg:"mountd access"; content:"|00 01 86 a5|";)
```

You can also use the IPS variables to specify the address:

```
alert ip !$HOME_NET $EXTERNAL_NET-> any any (ip_proto:igmp;)
```

Note.

If you specify any subnet as **$HOME_NET** and **$EXTERNAL_NET** — as **!$HOME_NET**, you cannot use an external subnetwork variable in the IPS protection because it leads to the error.

Port

You can specify port numbers of source and destination as the exact value, range, list or the **any** keyword (any port). To set the range, specify the upper and lower values divided by a colon (**:**). If one of border values is not

specified, the minimum (**0**) or maximum (**65535**) port number is used. Border values are included to the range.

The example of the IPS protection that reacts to all UDP packets sent to the ports in range from **0** to **1024** of the **class C 192.168.1.0** network:

```
drop udp any any -> 192.168.1.0/24 :1024
```

To form a list, separate ports by a comma. In this case and in case of using several port blocks, use highlighting symbols (**[]**).

The complement (**!**) is supported for the ports.

The example of the IPS protection that reacts to all TCP packets sent to any ports except X Window ports (**6000**–**6010**) and PostgreSQL (**5432**) and the **class C addresses (192.168.1.0)** network:

```
drop tcp any any -> 192.168.1.0/24 ![6000:6010, 5432]
```

Direction

Direction (**->** or **<>**) defines the traffic direction for the current IPS protection. Addresses and port to the left of this operator relate to packet source, to the right — to packet destination. You can also create bidirectional IPS protections with the help of (**<>**). In this case, each address-port pair means source as well as destination. You can use such IPS protections to analyze packets in session connections (for example, via POP3).

A bidirectional IPS protection example:

```
pass tcp !192.168.1.0/24 any <> 192.168.1.0/24 23
```

According to this IPS protection, all the packets directed from any address out of the **class C network (192.168.1.0)** to every IP address telnet port of the network and all the packets directed from telnet ports of **192.168.1.0/24** network IP addresses to other networks are passed.

<- cannot be used in IPS protections.

IPS protection options

The options are divided by a semicolon (**;**). Option keywords are separated from arguments by a colon (**:**).

There are four main categories of IPS protection options.

Category	Description
meta-data	Information about an IPS protection that has no impact on detection of packets and used counteractions
payload	Checks the content of packets (packet payload)
non-payload	Checks packet service fields
post-detection	Defines the action after meeting requirements of the IPS protection

For more information about IPS protection options, contact the technical support.

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Basics.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Deployment.