SECURITY code

Continent Enterprise Firewall
Version 4

Firewall

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

AD	Active Directory
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DMZ	Demilitarized zone
GMT	Greenwich Mean Time
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
IDN	Internationalized Domain Names
IP	Internet Protocol
MIME	Multipurpose Internet Mail Extensions
NTP	Network Time Protocol
OS	Operating System
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UTM	Unified Threat Management

Introduction

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

This document contains links to documents [**1**] – [**6**].

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
Overview

Firewall operation mode

The Firewall can operate in two modes:

- Standard mode — **UTM**;
- High performance mode — **High Performance FW**.

The Firewall interoperates with the Security Management Server, L2VPN, L3VPN, the Identification Agent and the Network Behavior Anomaly Detector.

When the Firewall is turned off in UTM mode, all filtering rules configured by the administrator stop working. A rule **Accept all** is created instead.

If you enable the IPS in UTM mode, all traffic will be transferred to the IPS on turning the Firewall off.

The high performance mode enables advanced traffic filtering and data transmission rate while performing basic tasks. The high performance Firewall supports interoperation only with the Firewall and QoS components and limits some features. The operation is only possible with an appropriate license.

In high performance mode, you can configure the number of cores used to process traffic on the Security Gateway.

Enable the Firewall

Standard mode

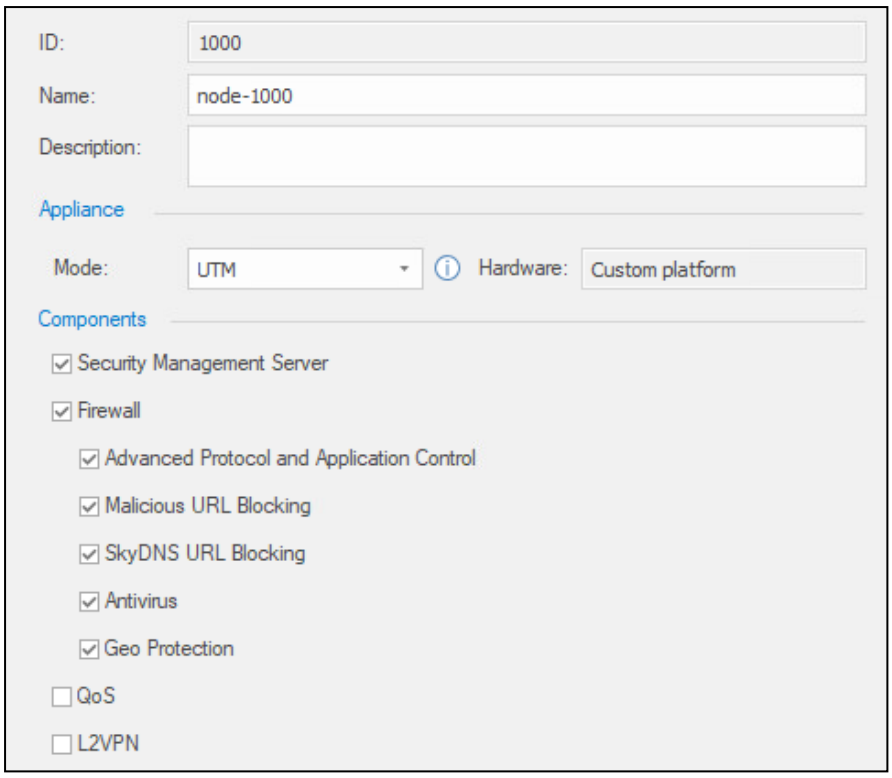
After you have deployed the Security Gateway, the **UTM** mode is set by default. The **Firewall** and **L3VPN** components are enabled by default.

After you have deployed the Security Management Server, the Security Management Server component is set by default.

To enable the Firewall in standard mode:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
2. Make sure that the **Mode** drop-down list value is set to **UTM**. In the **Components** group box, select **Firewall** and then select the components that must be functioning in the Firewall operation mode:
   - Advanced Protocol and Application Control;
   - Malicious URL Blocking;
   - SkyDNS URL Blocking;
   - Antivirus;
   - Geo Protection.

Attention!
To provide operation of the components above, the respective licenses are required.



Note.
You can select other components in **UTM** mode.

3. Click **OK**.

   The **Security Gateway** dialog box closes. The **Components** cell of the Security Gateway contains the **Firewall** icon .

4. After you have configured all the required parameters, save changes in the Security Management Server configuration and install the policy on the required Security Gateways.

If you disable the **Firewall** component, all custom firewall rules stop functioning. A rule that allows all packets is created instead.

If the **IPS** component is enabled on the Security Gateway and the Firewall component is disabled, all packets are sent to the IPS.

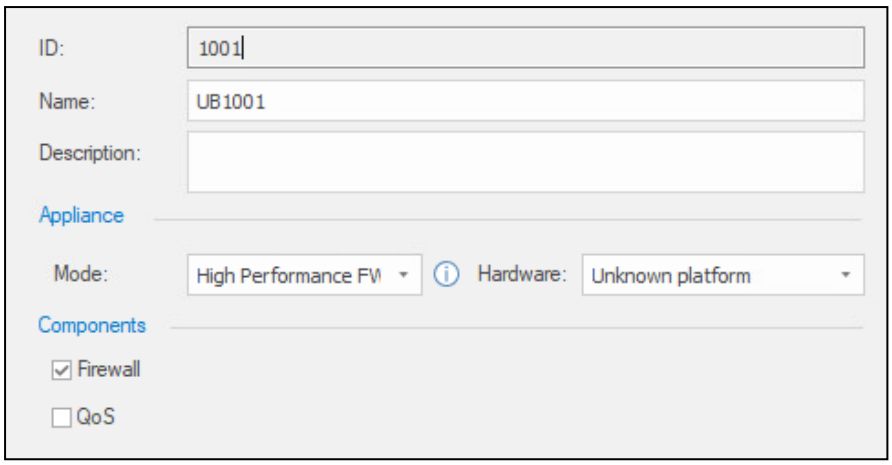
High performance mode

You can enable the high performance mode using either the Configuration Manager or the local menu. This mode is available only for hardware that supports the high performance mode. If the hardware does not support this mode, it cannot be selected in the Security Gateway properties in the Configuration Manager.

Attention!
Before starting the procedure, on the Security Gateway, in BIOS Setup, disable the **Hyper-Threading** mode.

To enable the Firewall in high performance mode using the Configuration Manager:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
2. In the **Mode** drop-down list, select **High Performance FW**.

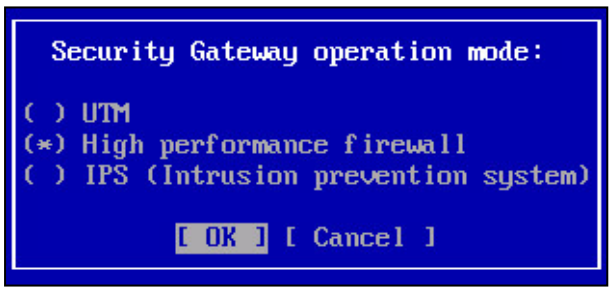


Note.
You can enable only **QoS** as an additional component in high performance mode.

3. Click **OK**.
   The **Security Gateway** dialog box closes.
4. After all the parameters are configured, save changes in the Security Management Server configuration and install the policy on the required Security Gateways.

To enable the Firewall in high performance mode using the local menu:

1. In the **Main menu**, go to **Settings | Security Gateway operation mode**.
   The **Security Gateway operation mode** dialog box appears as in the figure below.



2. Select **High performance firewall** and press **<Enter>**.
   The **Security Gateway operation mode** dialog box closes. You are returned to the **Settings** menu.
3. Select **Apply local policy** and press **<Enter>**.
   Wait for the procedure to complete.
4. Confirm changes from the Security Gateway on the Security Management Server. To do so, use the Configuration Manager or the local menu of the Security Management Server.
5. Reboot the Security Gateway using the Configuration Manager or the local menu of the Security Gateway.

Configure the number of cores used to process traffic

In High performance Firewall mode, you can configure the number of cores used to process the traffic. The table below shows the total number of cores, the number of cores available for traffic processing and the number of cores used by default depending on the platform.

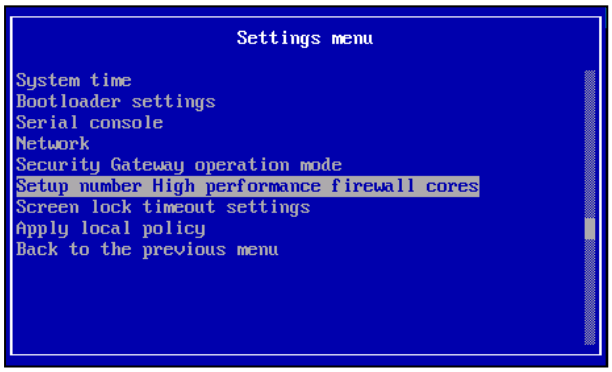
Platform	Total number of cores	Number of cores available for High performance FW	Used by default
IPC-1000NF2	4	2–3	2
IPC-3000F	14	3–12	8
IPC-3000NF2	14	3–12	8
IPC-R1000	6	2–5	5
IPC-R3000	8	2–6	6

You can configure the number of cores using the local menu of the Security Gateway.

To specify the number of cores used to process traffic:

1. In the local menu of the Security Gateway, select **Settings** and press <**Enter**>.

   The respective menu appears.

2. Select **Setup number High performance firewall cores** and press <**Enter**>.

   The dialog box prompting you to specify the number of cores appears.

   The dialog box also displays the number of cores reserved for traffic processing, its maximum value and default value.

3. Enter the required value and press <**Enter**>.

   After you press <**Enter**>, the script which makes changes to the system core and writes the respective value in the configuration file, starts running. Only the Security Gateway database stores this parameter. Thus, applying and sending policy to the Security Management Server is not required.

   The configuration will be applied after the Security Gateway reboot.

Chapter 2
Security Management Server objects

The Firewall is configured by creating access control rules.

The Firewall rules allow or deny incoming traffic. Thus, they enable control of access to either secure or external networks.

NAT rules modify IP addresses (ports) of transit packets.

The access control rules are grouped in lists in strict order. The list defines a sequence of actions on packets processed by Security Gateways. These lists are empty by default, and all the traffic is denied by the Security Gateway except the service packets.

Before creating the rules, you must create all the necessary Security Management Server objects that will be used as rule parameters.

Types of Security Management Server objects

The following Security Management Server objects are used to determine the packets to which the access control rules should be applied:

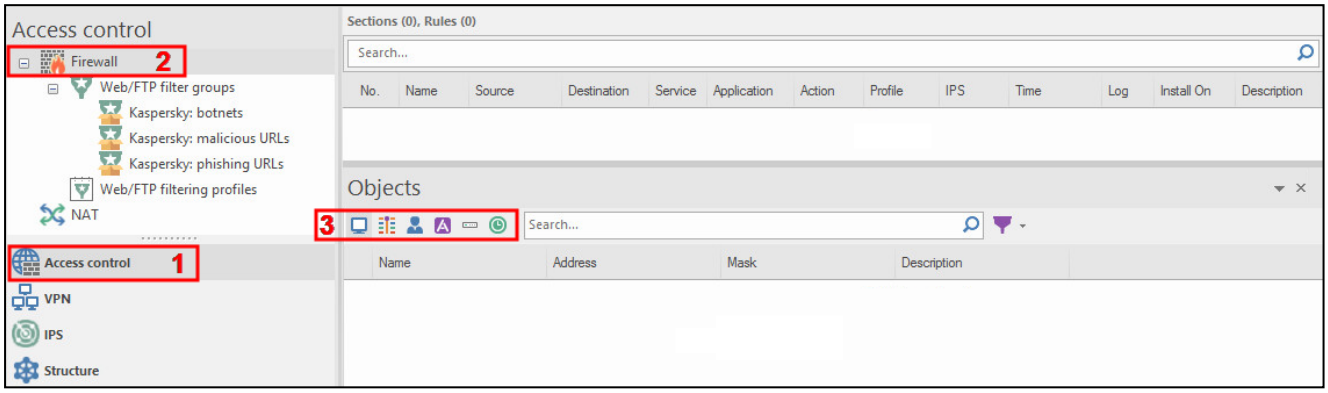
Objects		Description
Icon	Name	
	Network objects	The source or destination of the IP packet (the main parameter is an IP address or a range of the addresses)
	Services	Data transfer protocol
	Users	User of a protected network
	Protocols and applications	Protocols and applications which traffic can be detected
	Security gateways	Security Gateway where the rules will be installed
	Country	Country code of the IP packet sender/receiver
	DNS Name	DNS name of the IP packet sender/receiver
	Times	Time schedule for a rule
	QoS class	Traffic prioritization rules

Manage Security Management Server objects

To open the list of the Security Management Server objects:

- in the Configuration Manager, go to **Access control**, then select either **Firewall**, **NAT** or **Quality of service**.

  The Security Management Server objects are shown in the additional section. To select the required object type, click the respective button to the left of the **Search** text box.



Note.
The list of Security Management Server objects can be located in the toolbar (see [2], **Administering Configuration Manager**).

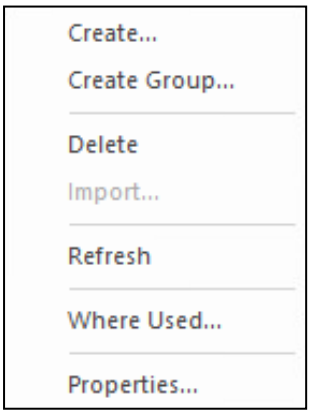
You can create, delete and configure the Security Management Server objects in this section.

You can perform the following operations with the Security Management Server objects:

- create a new object or a new group;
- delete an object;
- export or import an object;
- view the rules that use this object;
- view and configure the object parameters.

Note.
Some operations listed above are not applied to all objects.

To perform an operation, use the shortcut menu:



Note.
When working with lists in the CM, you can search for a required list element. The search can be performed using element attributes (Security Management Server object, interface, firewall rule, etc.). For this purpose, you need to type an attribute value or its part in the **Search** text box, then press <**Enter**>. You can also type logical expressions with ***and***, ***or***, ***not***, ***()*** in this text box.

For detailed information about how to manage the Security Management Server objects, see p. **31**.

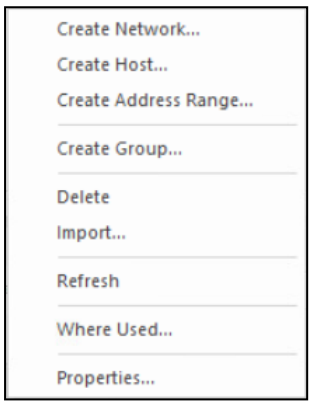
Network object

There are the following types of network objects:

	Host
	Network
	Address range
	Group of network objects

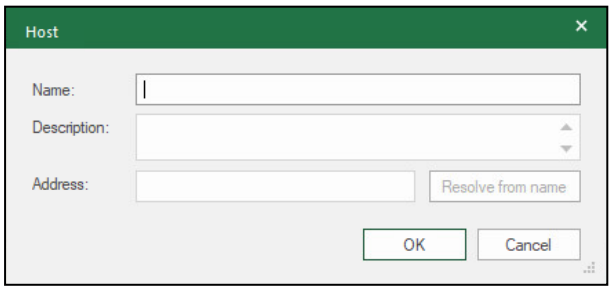
To create a network object:

1. Right-click the **Objects** area and select **Create...** with the required object type.

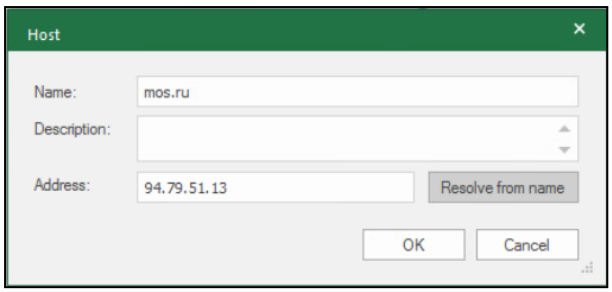


The dialog box prompting you to configure the network object appears as in the figure below.

2. Specify the parameters of the object:
   - for a network, in the **Address** text box, specify the IP address and the mask prefix (to edit the **Address** field, you can use the button to the right of this field).
   - for an address range, in the **Address** text box, specify the start and the end of the range using a dash (**-**).
   - for a host, the following window appears:



When creating a host, in the **Name** field, you can enter the IP address of a host, as well as its domain name (see the figure below). If you enter the latter, you can get the IP address by clicking the **Resolve from name** button. The IP address of a host appears in the **Address** field. For this purpose, DNS servers that are configured on the computer with the Security Management Server are used.



Note.
If DNS servers are not available, an error message will appear.

3. Click **OK**.

   The new object appears in the **Objects** section.

4. After you have configured all the required parameters, save the changes on the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

Attention!
You can import network objects from a **.txt** file automatically (see p. **85**).

To edit the parameters of a network object:

1. Open the list of objects.
2. Right-click the required object and click **Properties**.

   The dialog box where you can configure the network object appears.

3. Modify the required parameters, then click **OK**.

   The object parameters are changed and displayed on the list.

4. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To delete a network object:

Attention!
Before deleting an object, you must remove it from each rule that uses this object. To find out the rules where this object is used, right-click it in the Security Management Server object list and select **Where Used...**. The list of rules will be displayed.

1. Open the list of objects.
2. Right-click the required object and click **Delete**.

   A dialog box asking you to confirm the action appears.

3. Click **Yes**.

   Note.
   If the object is used in active access control rules, a dialog box containing an error message and a list of affected rules appears. Otherwise, the object will be deleted.

4. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

Service

Services are categorized respectively with the used protocol:

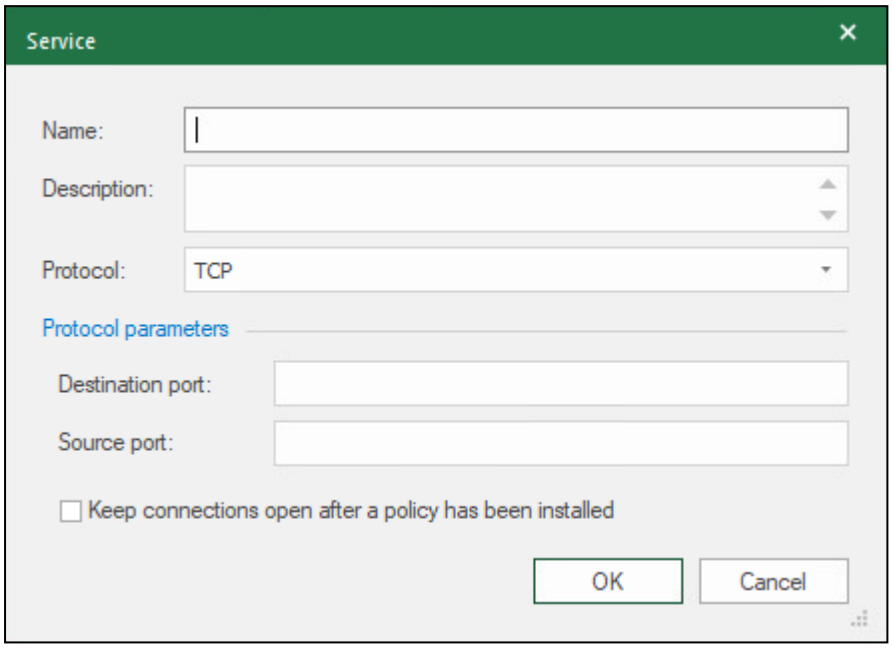
	ICMP services
	IP services
	TCP services
	UDP services
	A group of multiprotocol services

After Continent installation, the list of preinstalled servers with specified parameters is stored in the Security Management Server Database. An administrator can change these parameters and create new ones.

To create a service:

1. In the **Objects** area, click **Services**, then right-click the list of the services and click **Create**.

   The dialog box prompting you to configure the service parameters appears as in the figure below.



2. You can configure the following service parameters:

Parameter	Description
Name	The name of the service must be informative and brief because the list displays only its icon and name
Description	Detailed information about the service
Protocol	Used protocol. Select it from the drop-down list or enter its number. For example, if you enter 47, the GRE protocol is identified automatically
Protocol parameters	Configure parameters that are specific for the selected protocol: • for TCP and UDP – specify the source and destination ports of IP packets. To do so, in the drop-down list, select the required parameter for both the source and the destination; then, in the appeared text box, type the port number (range). For example, **132, 45322-45819, 655354**; • for ICMP – select the type of ICMP message from the drop-down list. Also, you can specify a message code for the following types: **03 Destination unavailable, 05 Redirect, 11 Time exceeded, 12 Parameter problem**
Keep connections open after a policy has been installed	If the check box is not selected, the connection state for the specified service after the policy is applied will be defined by the settings configured for the Security Gateway (see p. **74**). If the check box is selected and the **Rematch connections** value is set in the settings for the Security Gateway (see p. **74**), the connection for this service will not be closed

3. Click **OK**.

   You can see the new service data in the list in the **Objects** section.

4. After all the parameters are configured, save changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To configure the service parameters:

1. In the **Objects** area, select **Services**.
2. Right-click the required service and select **Properties**.

   The dialog box for configuring the service parameters appears. A set of displayed fields depends on the selected protocol.

3. Modify the required parameters.
4. Click **OK**.

   You can see the changes in the list of services.
5. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To delete a service:

> **Attention!**
> Before deleting a service, you must remove it from each rule that uses this object. To see which **Firewall**/**NAT** rules use the service, right-click the required service in the list of Security Management Server objects and select **Where Used** in the shortcut menu. The list displaying the number and name of the rule appears.

1. In the **Objects** area, select **Services**.
2. Right-click the required service and select **Delete**.

   The dialog box prompting you to confirm the action appears.
3. Click **Yes**.

   The service will be deleted.

   > **Attention!**
   > If active **Firewall**/**NAT** rules use the required service, an error warning with the list of rules using the service appears.
4. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

User

The **Users** objects are used to set the source value in the Firewall rules. You can create these objects manually or import them from Active Directory.

You can also group users. The groups can also be used in the **Firewall** and **Remote access** rules as the source. A group can be included in another group.

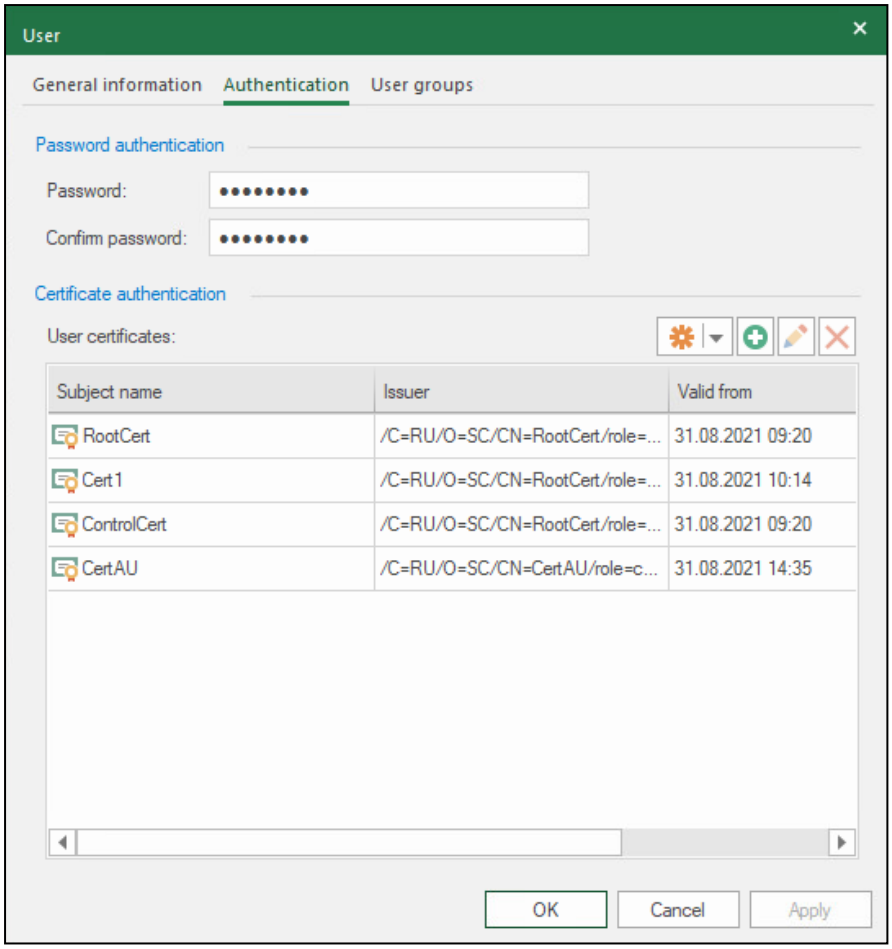
To create a user account:

1. In the **Objects** area, select **Users**, then right-click the list of users and select **Create**.

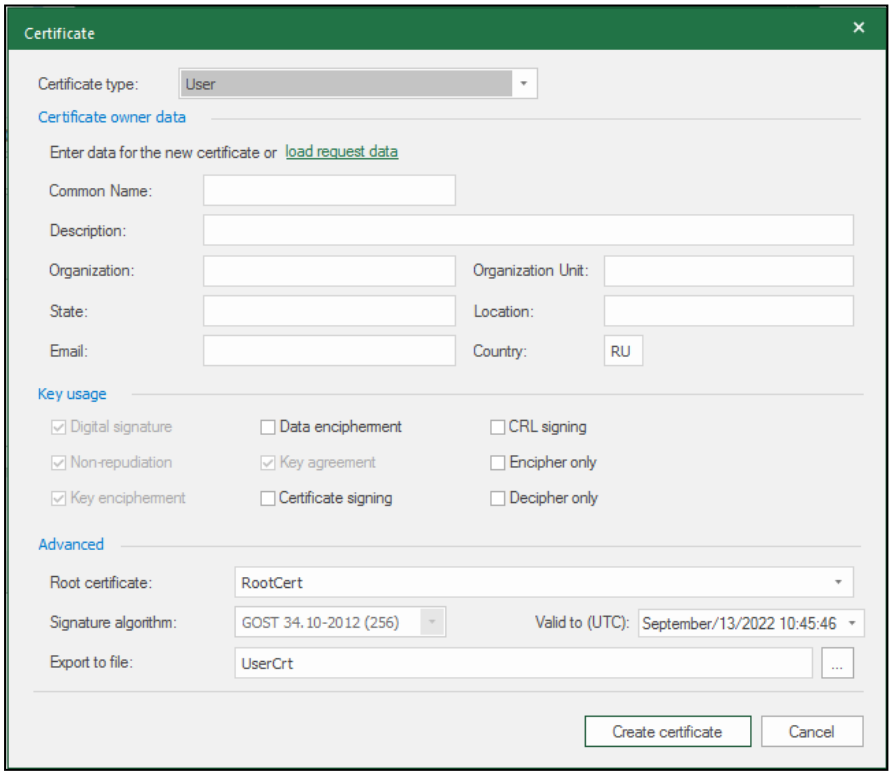
   The dialog box prompting you to configure the parameters appears.
2. Configure the user account parameters on the **General information** tab:

Parameter	Description
Login	A login must be informative and brief because the list displays only the login itself and the icon
Full name	Last, first and middle name of the user
Description	Advanced information about the user
Email	Email address of the user
Organization	Employment information about the user
Position	
Block the account	When the check box is selected, the user cannot access resources of the secure network

3. Go to the **Authentication** tab and specify the required data. For certificate-based authentication, click  and select the required certificate.



4. If a proper certificate is missing or you need to create a new one, click **Create Certificate** .
The **Certificate** dialog box appears.



5. Enter the required information in the text boxes and click **Create certificate**.
The entropy collection process of the RNG starts.

Wait for the entropy collection process to complete, then finish the user certificate creation.

6. After you have added the user certificate to the list, click **OK**.

   The created user is added to the list of users.

7. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To configure parameters of a user account:

1. In the **Objects** area, click **Users**.
2. Right-click the required user and click **Properties**.

   The dialog box where you can configure the user account appears.

3. Configure the required parameters and click **OK**.

   You can see the changes in the list of users.

4. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To delete a user account:

Attention!
Before deleting a user, you must remove it from each rule that uses this object. To find out which rules the user has included, right-click the required user in the list of Security Management Server objects and select **Where Used**. The list displaying the number and name of the rule appears.

1. In the **Objects** area, click **Users**.
2. Right-click the required user and click **Delete**.

   The dialog box prompting you to confirm the action appears.

3. Click **Yes**.

   The user account is deleted.

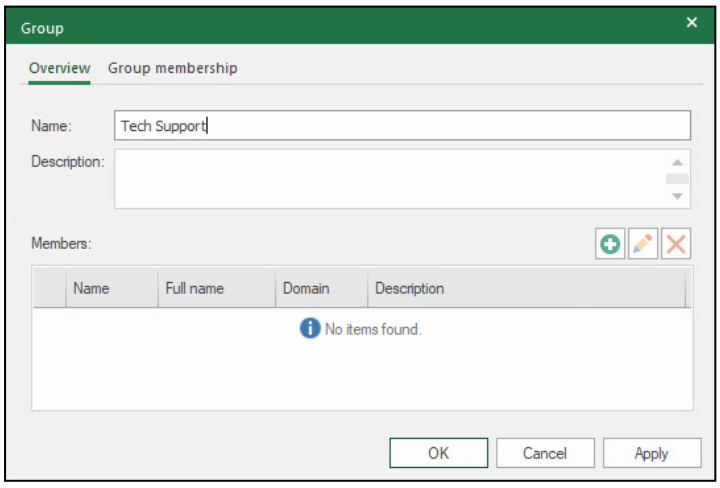
   Attention!
   Before deleting, exclude a user from firewall rules or remote access rules. To find out in which rules a user is used, select the required user in the Security Management Server object list, right-click it, and select **Where Used**. A list with the number and name of the rule appears.

4. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways.

To create a group of users:

1. In the **Objects** area, select **Users**, right-click the list of users, then select **Create group** in the shortcut menu.

   The **Group** dialog box appears as in the figure below.



2. In the **Name** and **Description** text boxes, enter the respective information.
3. To add users or groups, click .

   The list of users and groups appears.

Note.
If the list is empty, you can create the required objects or groups. To do so, click **Create**.

4. Select the required users or groups and click **OK**.
   The selected users are added to the group.
5. Click **OK**.
   The **Group** dialog box is closed and the new group appears in the list of objects.
6. Save changes in the Security Management Server configuration.

To add a user/group to a group:

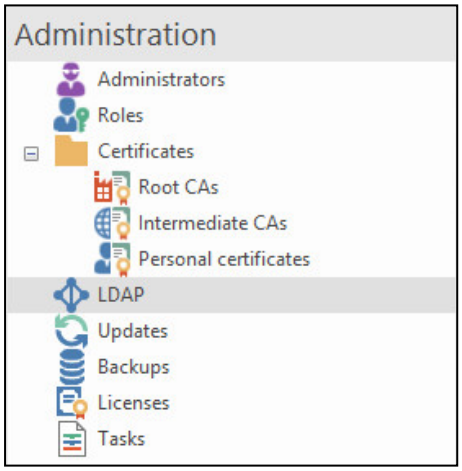
1. In the **Objects** area, select **Users**, right-click the required group and select **Properties** in the shortcut menu.
   The **Group** dialog box appears.
2. Click and in the appeared dialog box, select the required users or groups, then click **OK**.
   The selected objects are added to the group.
3. Save the changes in the Security Management Server configuration.

Note.
You can see added users or groups in the **User** dialog box, the **User groups** tab or the **Group** dialog box, the **Group membership** tab.

To import user accounts from Active Directory:

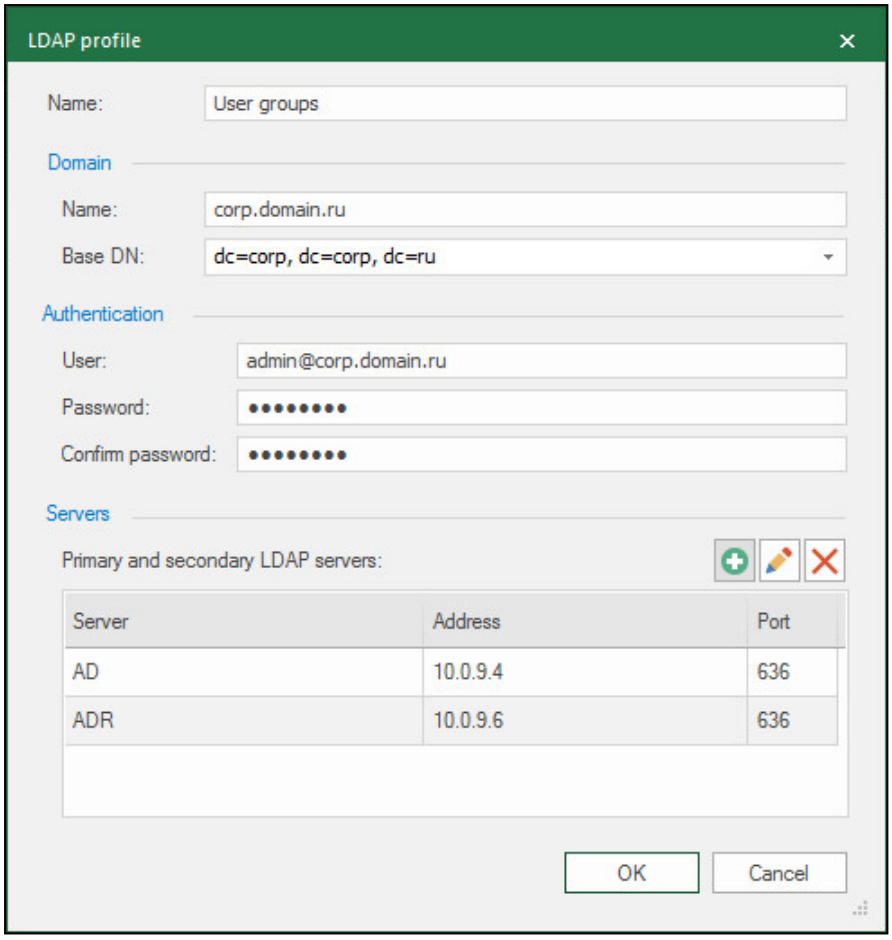
Attention!
The following procedure can be performed only if there is a connection between the Security Management Server and LDAP server.

1. In the Configuration Manager, select **Administration** and click **LDAP**.



   The LDAP profiles list appears in the display area.
   If LDAP profiles have not been created, the list is empty. In this case, go to step **2**.
   If a required profile is on the list, go to step **9**.
2. On the toolbar, click **LDAP**.
   The **LDAP profile** dialog box appears.

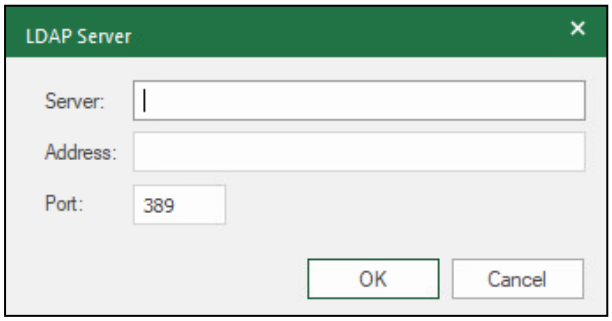
Note.
By default, the **LDAP profile** dialog box parameters are empty.



3. Specify the required information in the respective text boxes:

Parameter	Description
Name	Profile name
Domain	
Name	Name of the domain from which you need to import user accounts
Base DN	Directory branch from which a user account search starts. Using spaces between Base DN components is not allowed
Authentication	
User	User that has access to Active Directory
Password/Confirm password	Password of the user

4. In the **Servers** group box, specify the master and reserve LDAP server. To do so, click .
The dialog box appears as in the figure below.



5. Specify the name and address of the server. Both parameters are required. There are no restrictions for specifying the server name. You should specify an IPv4 address or server domain name in the **Address** text box.

   If necessary, modify the port number.

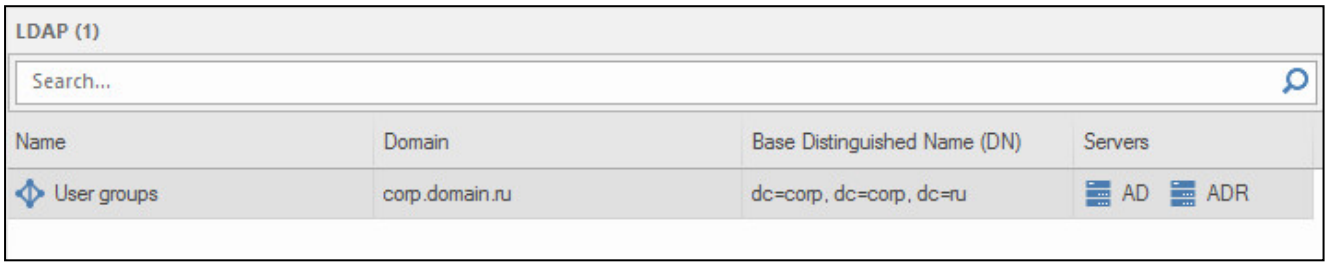
6. Click **OK**.

   The server is added to the list.

7. Repeat step **5** for the reserve server.

8. In the **LDAP profile** dialog box, click **OK**.

   The created profile appears in the list.



9. In the display area, select the required profile and click **Import** on the toolbar.

   The system starts connecting to the LDAP server. The **Importing LDAP groups** dialog box appears.

   LDAP groups available for import appear in the list.

10. Select the required groups and click **Import**.

    The system starts importing the selected groups. When the action is finished, the respective message appears.

11. Click **OK**.

12. Go to the list of users.

    The list of users now contains user groups imported from Active Directory.

> **Attention!**
> The Configuration Manager starts to work slower if there are too many AD groups. We recommend using Active Directory nested groups.

13. Save the changes in the Security Management Server configuration.

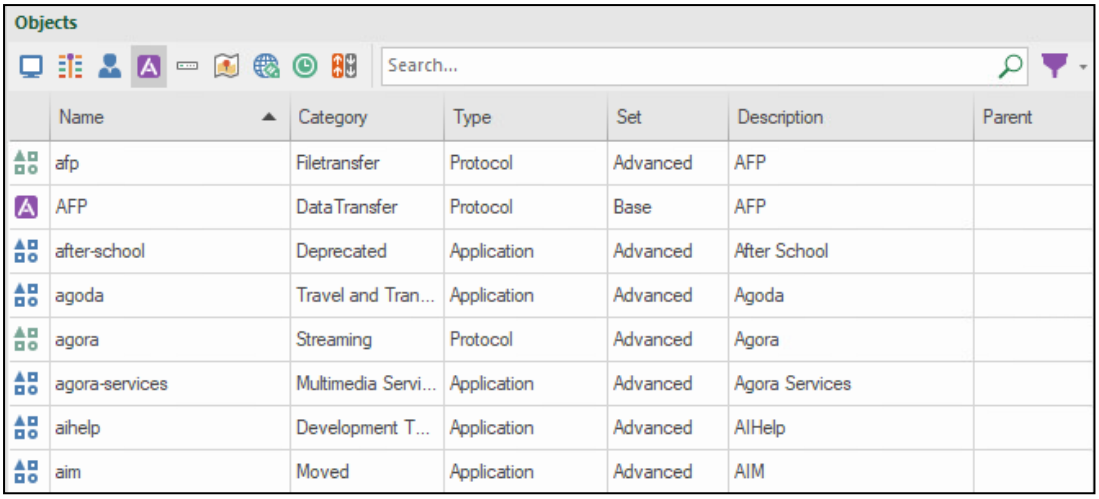
Protocols and applications

Basic application control

Vendor application signatures are divided into categories. You cannot delete, edit or add the signatures.

There are the following application categories:

- Authentication;
- Business applications;
- Cloud storage;
- Email;
- File transfer;
- Hidden data transmission;
- Message exchange;
- Network functions;
- P2P networks;
- Remote access;
- Social networks;
- Streaming;
- Virtualization;
- Voice communication.



Name	Category	Type	Set	Description	Parent
afp	Filetransfer	Protocol	Advanced	AFP	
AFP	DataTransfer	Protocol	Base	AFP	
after-school	Deprecated	Application	Advanced	After School	
agoda	Travel and Tran...	Application	Advanced	Agoda	
agora	Streaming	Protocol	Advanced	Agora	
agora-services	Multimedia Servi...	Application	Advanced	Agora Services	
aihelp	Development T...	Application	Advanced	AIHelp	
aim	Moved	Application	Advanced	AIM	

Advanced application control

To use advanced application control, upload additional application signatures to the Security Management Server database. If necessary, you can create a custom signature by copying an existing one and editing its parameters.

Security Gateway

Security Gateway objects are divided into the following types:

	Security Management Server
	Security Gateway
	A group of Security Gateways
	Security Cluster

To create a Security Gateway:

1. In the **Objects** area, select **Security gateways**, right-click the list of Security Gateways and select **Create** in the shortcut menu.

   The dialog box prompting you to configure the Security Gateway parameters appears.
2. For detailed information about the Security Gateway creation, see [**1**].

To configure parameters of a Security Gateway:

1. In the **Objects** area, select **Security gateways**.
2. Right-click the required Security Gateway and click **Properties**.

   The dialog box for configuring the Security Gateway parameters appears.
3. Configure the required parameters (see [**2**]) and click **OK**.
4. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To delete a Security Gateway:

1. In the **Objects** area, select **Security gateways**, right-click the required object and select **Delete**.

   The dialog box prompting you to confirm the action appears.
2. Click **Yes**.

   The Security Gateway is deleted.

   Attention!
   If active rules use the Security Gateway required to delete, an error warning with the list of rules using the Security Gateway appears.
3. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways.

Country

The Security Management Server object **Countries** makes it possible to use the geographical affiliation of source and destination IP addresses as a packet filtering criterion.

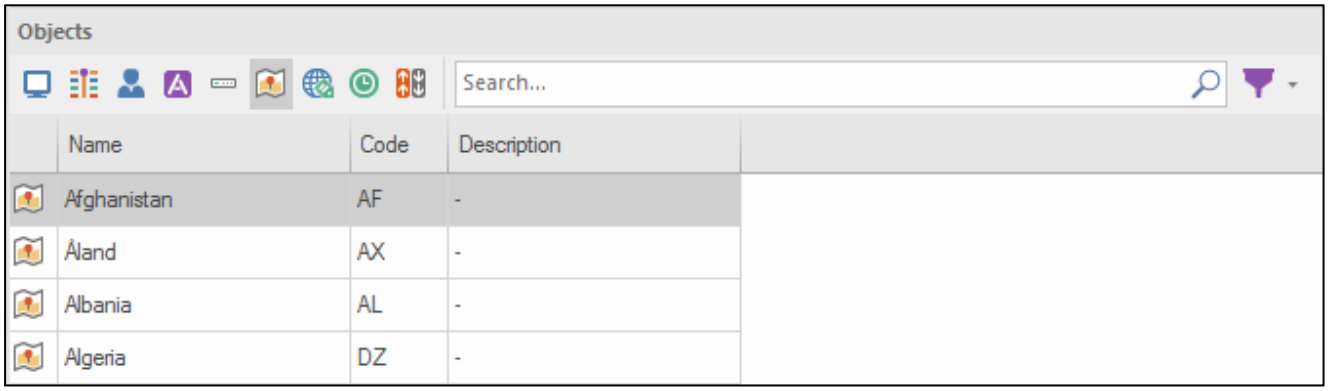
Attention!
To use IP addresses geographic identity, enable **Firewall** and **Geo Protection** mode on a Security Gateway (see p. 7).

The pre-installed list of **Countries** objects is stored in the Security Management Server Database and is updated by an administrator with a given frequency.

You can create **Group** objects, to which you can add countries from the pre-installed list and the groups created earlier. The **Group** object as well as **Countries** can be used as sources or destinations in the Firewall rules.

To view the Countries list of objects:

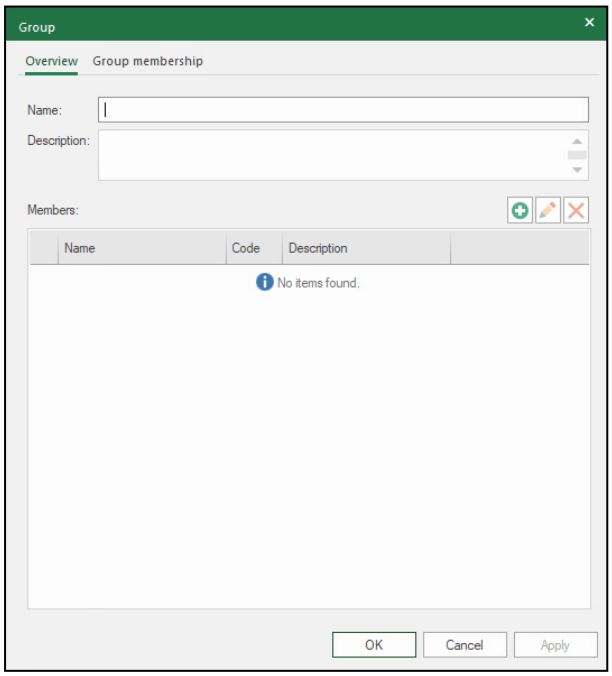
1. In the Configuration Manager, go to **Access control | Firewall**.
2. In the **Objects** area, select **Countries**.
   The list of countries and their codes appears.



   The list is not available for editing.

To create a group of countries:

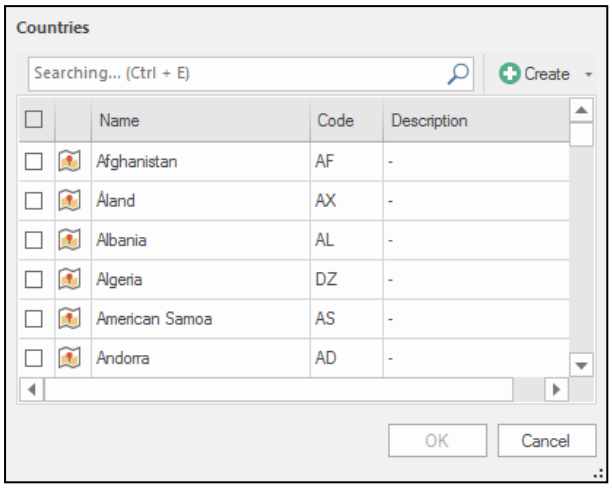
1. Right-click the **Objects** area and select **Create Group**.
   The **Group** dialog box appears.



2. On the **Overview** tab, specify **Name** and **Description**.
3. Add new members. To do so, click  .

The list of countries appears.

Note.
If you created groups of countries, they are also displayed.



4. Select the required countries and/or groups and click **OK**.
   The selected countries and groups are displayed on the **Overview** tab.
5. In the **Group**, click OK.
   The **Group** dialog box closes and the new group appears at the end of the **Countries** list.

You can perform the following operations with groups of countries:

- delete a group;
- edit a group (edit a name or a description, add or delete elements).

To delete a group:

1. In the **Countries** list, right-click the group you want to delete and click **Delete**.
   A dialog box prompting you to confirm the action appears.
2. Click **Yes**.
   The group is deleted.

To edit a group:

1. In the **Countries** list, right-click the group you want to edit and click **Properties...**.
   The **Group** dialog box appears.
2. If necessary, edit **Name** and **Description**.
3. To edit the group members, use **Add**, **Properties** or **Delete** buttons.
4. After you finish editing, click **OK**.
   The **Group** dialog box closes.

DNS name

The Security Management Server object **DNS Names** is used as a source and a destination in the Firewall, NAT and QoS rules. In Continent, only defined domain names (FQDN) are used as names.

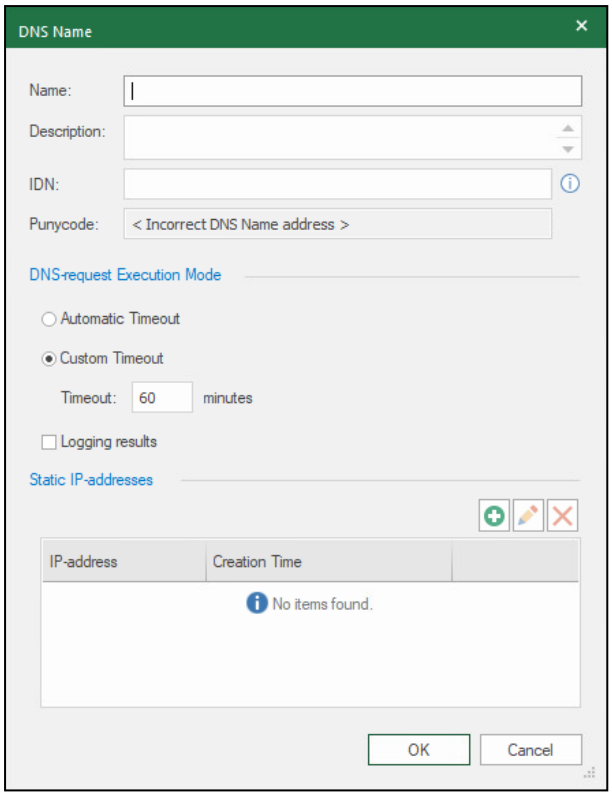
You can create DNS name groups, to which you can add **DNS Names** objects and the groups created earlier. The DNS Name groups as well as the **DNS Names** object can be used as a source or a destination.

Note.
To use these objects, configure the DNS service in the Security Gateway properties (see [**5**]).

To create a DNS Name object:

1. In the Configuration Manager, go to **Access Control | Firewall**.
2. In the Objects area, select **DNS Names**.
   The list of objects appears. If the objects were not created earlier, the list is empty.
3. Right-click the Objects area and select **Create**.

The **DNS Name** dialog box appears.



4. Specify **Name** and **Description**.
5. In **IDN**, enter a resource URL address.

   After specifying the URL, **Punycode** is entered automatically.
6. Select the **DNS-request Execution Mode** parameter — automatic or custom.
   - if you select **Automatic Timeout**, the update time value is received from an external DNS server.
   - if you select **Custom Timeout**, specify **Timeout** value in minutes. The minimum value — **1** minute. The maximum value — **10,800** minutes (7 days).
7. If the event registration is related to this object, select **Logging results**.

Attention!
Registration will be performed in the system log.

8. If the resource static IP addresses are known, enter them using  .
9. Click **OK**.

   The **DNS Name** dialog box closes and the created object appears.

You can perform the following operations with the **DNS Names** objects:

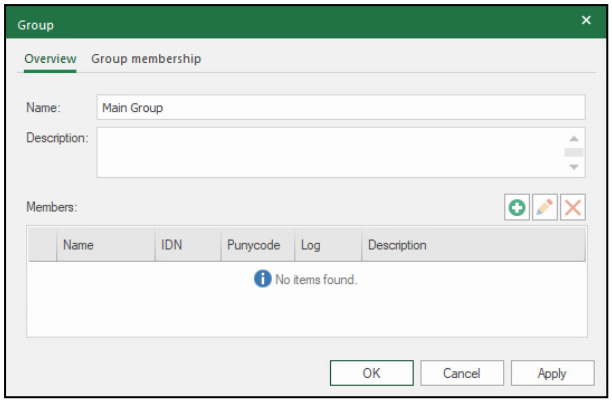
- delete;
- edit parameters (edit parameters specified while creating the object).

To perform the operations above, right-click an object in the list and use the commands.

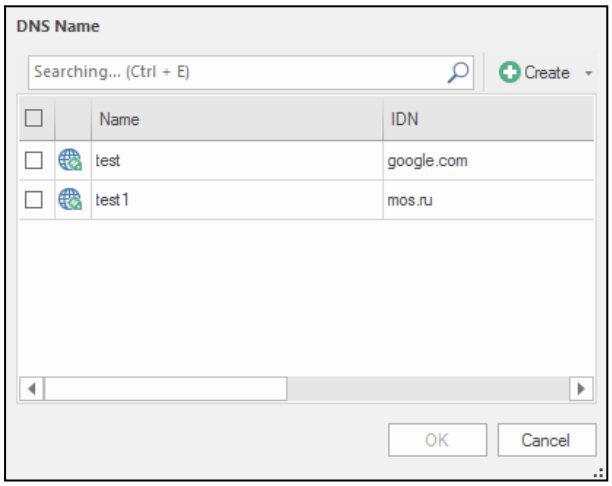
To create a group of DNS names:

1. In the **DNS Names**, right-click and select **Create Group**.

   The **Group** dialog box appears.



2. On the **Overview** tab, specify **Name** and **Description**.
3. Add members to the group. To do so, click .
   The list of **DNS Name** objects appears.



4. Select the required objects and click **OK**.
   The selected DNS names and groups appear in the list in the **Overview** section.
5. In the **Group** dialog box, click **OK**.
   The **Group** dialog box closes and the new group appears at the end of the **DNS Names** list.

You can perform the following operations with groups:

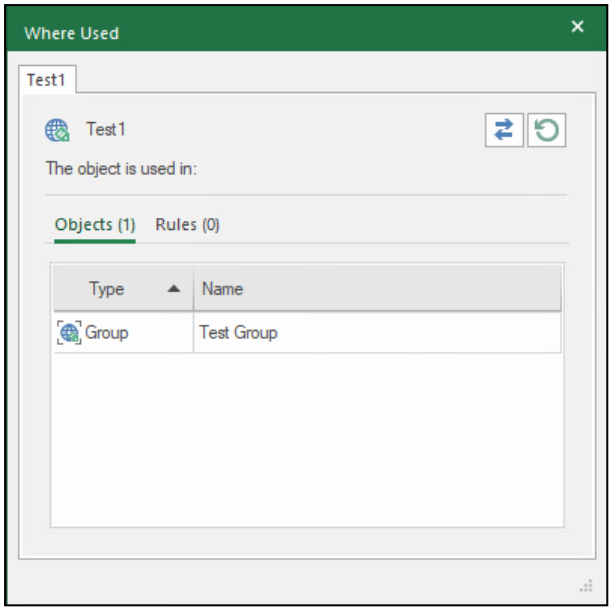
- delete a group;
- edit a group (edit a name and a description, add or delete elements).

To perform the operations above, right-click a group in the list and use the commands.

You can view the usage of **DNS Names** objects and groups in rules or groups.

To view where the DNS Names object is used:

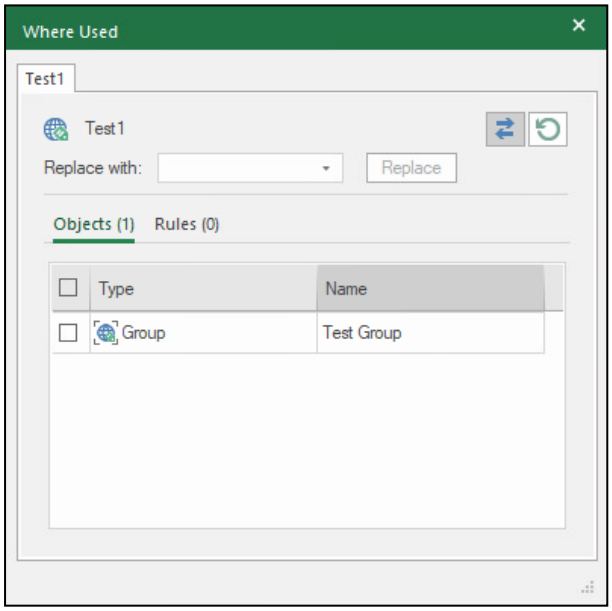
1. In the **DNS Names** list, right-click an object and select **Where Used...**.
   The **Where Used** dialog box appears.



On the **Objects** tab, a group or groups where the object is located are displayed. On the **Rules** tab, the rules in which the object is used are displayed.

2. If you need to replace one object with another one, click the **Replace mode** button .

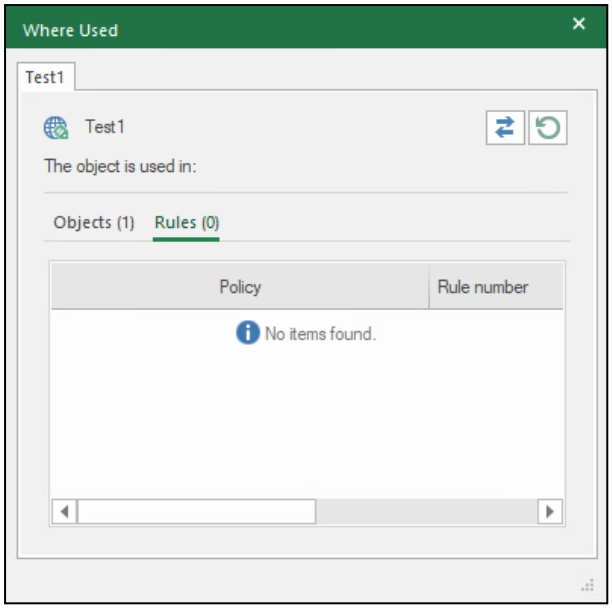
   The **Where Used** dialog box looks like the figure below.



3. On the **Objects** tab, select the group in which you want to replace the object.
4. In **Replace with**, select the object from the drop-down list.
5. Click **Replace**.

   A dialog box prompting you to confirm the action appears.
6. Click **Yes**.

   The object will be replaced.
7. In the **Where Used** dialog box, go to the **Rules** tab.



The list of the rules in which the object is used is displayed.

The following parameters are provided for each rule:

- Policy (firewall, NAT rules, QoS, remote access rules);
- Rule number;
- Role (source/destination);
- Rule.

8. If you need to replace one object with another one, click the **Replace mode** button and take steps **2–6**.
9. After the viewing, close the **Where Used** dialog box.

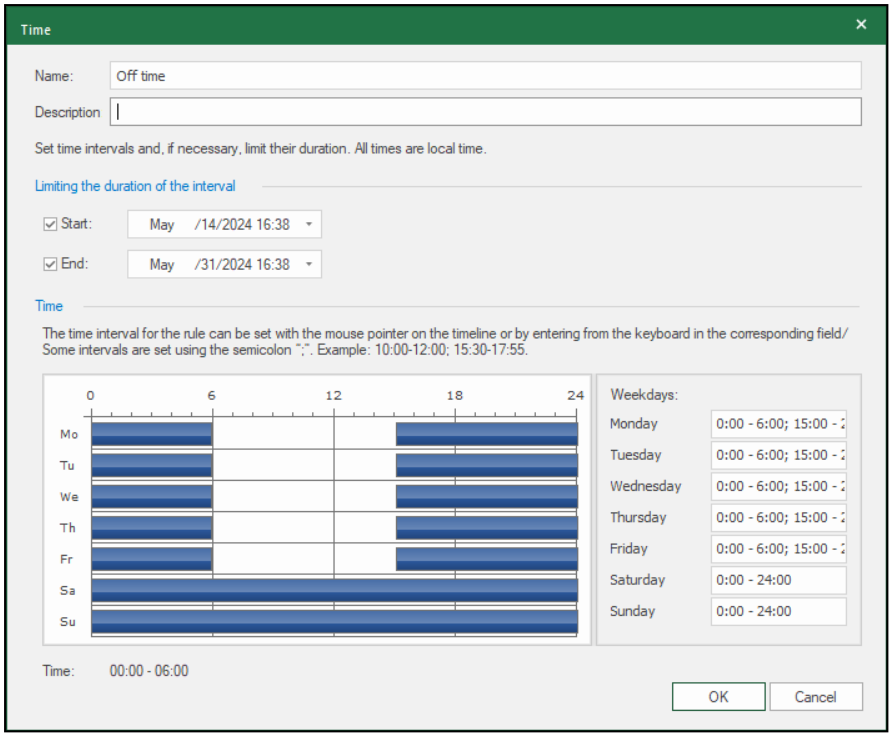
Time

To create a time interval:

1. In the **Objects** area, select **Times**, right-click the list of objects and select **Create**.

   The dialog box prompting you to configure the time appears.
2. In the **Name** text box, enter a name for this schedule; in the **Description** text box, enter some additional information about it.

   Note.
   We recommend giving informative names because you can only see the names of schedules while configuring filtering rules.
3. Specify the start and end dates of the interval duration.
4. Specify the schedules for the access control rules: point to the beginning of the time interval, hold the mouse button and drag the pointer to the end of the interval. To specify another interval, repeat the procedure. You can also enter the time for the start and the end of the interval using the dash (**-**) between them and the semicolon (**;**) between different time intervals of the same day of a week.



Note.
The time configured for the time intervals is **UTC**. So, when configuring the time intervals, take into account the time difference for the time zone of Firewall rules.

5. Click **OK**.

   You can see the new time interval data in the list in the **Objects** area.

6. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To configure the parameters of a time interval:

1. Open the list of the objects, right-click the required time interval and select **Properties** in the shortcut menu.

   The dialog box where you can configure the time appears.

2. Modify the required parameters, then click **OK**.
3. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

To delete a time interval:

Attention!
Before deleting a time interval, you must remove it from each rule that uses it. To see which rules use the time interval, right-click it in the list of Security Management Server objects and select **Where used** in the shortcut menu. The list displaying the number and name of the rule appears.

1. Open the list of objects, right-click the required time interval and click **Delete**.

   The dialog box prompting you to confirm the action appears.

2. Click **Yes**.

   The time interval is deleted.

   Attention!
   If active rules use the required time interval, an error warning with the list of rules using the interval appears.

3. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

QoS class

After the Continent OS has been installed, the list of the following QoS classes is created in the Security Management Server Database:

Name	Description
Best Effort	Undifferentiated applications
Call Signalling	SCCP, SIP, H.323
Critical Data	ERP Apps, CRM Apps, Database Apps, E-mail, FTP, Backup Apps, Content Distribution
Interactive Video	Video presentation
Network Control	OAM&P, EIGRP, OSPF, BGP, HSRP
Scavenger	YouTube, iTunes, BitTorent, Xbox Live, eDonkey
Streaming Video	VOD servers
Voice	IP telephony

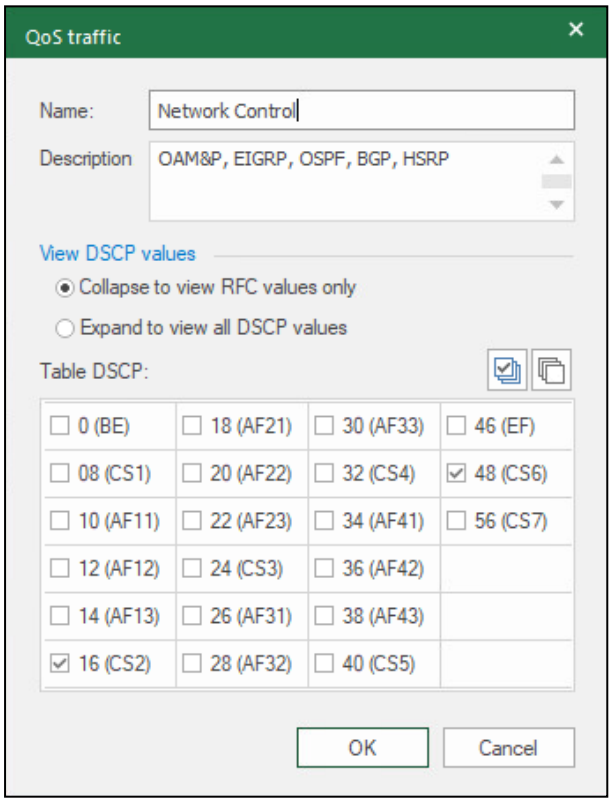
These QoS classes can not be deleted.

You can edit the parameters, create new classes and add them to the list.

To view and edit the class parameters:

1. Select the class, right-click and select **Properties**.

   The dialog box, where you can configure the parameters, appears.



   The class name, its description and DSCP values are displayed.

2. If you need to edit the DSCP values, select or clear the respective check boxes. The standard set of values is displayed by default.

   If you need to use an expanded set of values, select **Expand to view all DSCP values**, then select the required check boxes.

3. Click **OK**.

   The dialog box closes.

To create a new QoS class:

1. In the display area, right-click and select **Create**.

   The dialog box, where you can configure the parameters, appears (see above).

2. Enter a class name and its description.

3. Specify the DSCP value, using a standard or expanded set of values.

   Click **OK**.

   The created class appears in the list.

To delete a QoS class:

> **Attention!**
> Before deleting an object, you must remove it from each rule that uses this object. To find out the rules where this object is used, right-click it in the Security Management Server object list and select **Where Used...**. The list of rules will be displayed.

1. Go to the QoS class list.
2. Right-click the required object and select Delete.

   The dialog box prompting you to delete the object appears.
3. Click **Yes**.

   The object will be deleted from the QoS class list.

   > **Attention!**
   > If the deleted object is used in the active rules, the respective message appears.
4. Save configuration and install policy on the required Security Gateways.

Manage groups

You can combine objects into groups for convenient display and management. You can combine the following objects types:

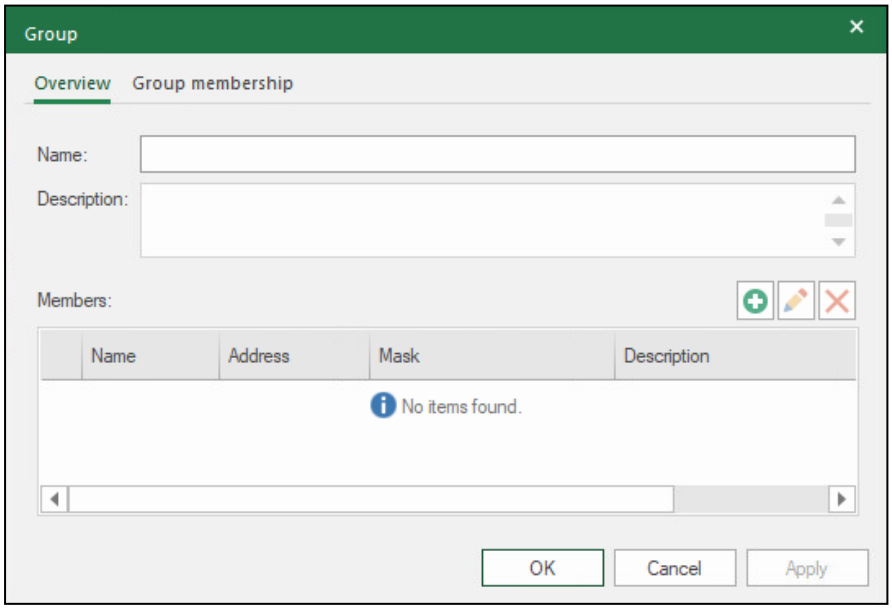
- network objects;
- services;
- users;
- applications;
- Security Gateways;
- DNS Names;
- countries.

The objects included in a group are not deleted when the group is deleted.

To create a group:

1. In the additional dialog box of Security Management Server objects, select the object type, then select **Create group** in the shortcut menu.

   The respective dialog box appears.



2. Specify the required parameters and click **OK**:

Parameter	Description
Name	Name of a group
Description	Additional information (optional)
Members	Set of objects included in a group. To add and remove objects from a group, use and . To edit parameters of the added object, select it and click

The data of the new group appears in the **Objects** area.

3. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. 84).

To edit a group:

1. In the **Objects** area, right-click the list of objects and select **Create group** in the shortcut menu.

   The respective dialog box appears.
2. Edit the required parameters and click **OK**.
3. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. 84).

To delete a group:

Attention!
Before deleting an object, you must remove it from each rule that uses this object. To find out the rules where this object is used, right-click it in the Security Management Server object list and select **Where Used**. The list of rules will be displayed.

1. Right-click the required group and select **Delete** in the shortcut menu.

   The dialog box prompting you to confirm the action appears.
2. Click **Yes**.

   The group is deleted and removed from the list. This action does not delete objects included in the group.

   Attention!
   If the group is used in the active rules, the respective message appears.
3. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. 84).

Chapter 3
Firewall rules

Firewall rule parameters

The list of rules contains the following parameters:

Parameter	Description
№	Unique number of a rule in the list. Used as an ID in logs
Name	Name of a rule
Source	Source IP address. Displays the name of a network object/group of network objects or a user/group of users, country, DNS name
Destination	Destination IP address. Displays the name of a network object/group of network objects, country, DNS name
Service	Set of controlled services/group of services
Protocol/Applications	Set of controlled applications/group of applications
Action	Action to apply to IP packets: • **Accept** — to allow packets or send them to the other components (WEB/FTP filters or the IPS) for further processing; • **Drop** — to deny incoming packets; • **Filter** — to define an action by WEB/FTP profile
Profile	Active WEB/FTP filtering profile (see p. **51**)
IPS	This parameter determines whether a processed packet is sent to the IPS component signature analyzer: • **On** — traffic is sent to the IPS component; • **Off** — traffic is not sent to the IPS component
Time	Schedule for the rule operation (according to the UTC standard)
Log	Record of rule action in the network security log. If packets are sent to the IPS component, the log contains both the Firewall and the IPS events. The IPS events are logged regardless of this parameter
VRF	VRF zones in which this rule must work. You can specify the zone only if a single Security Gateway is specified in **Install On**
Install On	Set of the Security Gateways to which the rule is applied
Description	Description of a rule

Attention!
When you specify the **Source** and **Destination** parameters, you can select **Negate cell** in the shortcut menu. This means all possible values except the one specified in this cell.

Manage Firewall rules

Firewall rules are applied in strict order (from first to last). If an IP packet complies with the rule parameters, the packet is processed according to the selected action. This packet will not be processed again.

Note.
The 5-tuple Firewall rule parameters are bound together by the **AND** logical operator.

To manage the list of rules, you can use its properties or the buttons on the toolbar.

Attention!
The properties and the list of commands are unique for each parameter.

While creating rules, take into account that transit traffic cannot pass through Security Gateways by default. The service packets are the only exception. Events of the packets drop are not logged by default. If you disable the Firewall, all custom Firewall rules stop functioning. A rule that accepts all packets is created instead.

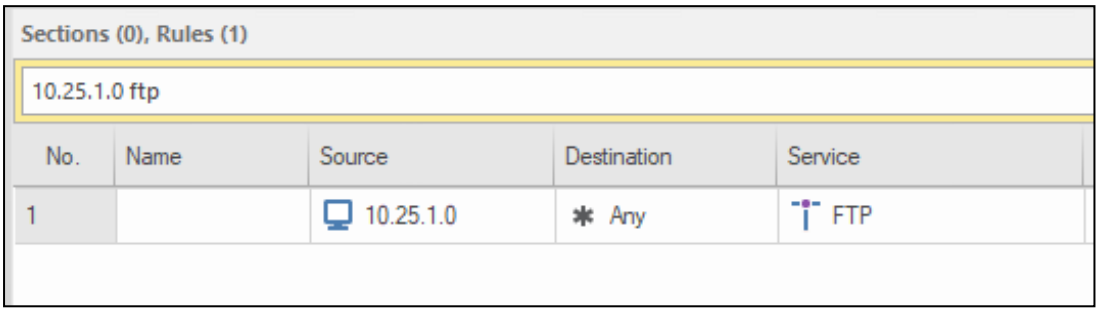
To open the list of Firewall rules:

- in the Configuration Manager, go to **Access control** | **Firewall**.

  The list of Firewall rules for IP packets appears.

The list is displayed as a table where each line is a single rule.

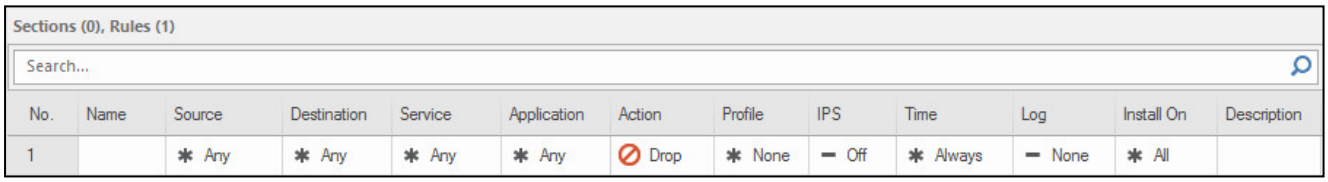
You can search for a rule by its attributes. To do so, in the search bar, type space-separated attributes, for example, **10.25.1.0 ftp** (see figure below).



To create a rule:

- in the list of rules, right-click the **No.** column and click the respective command for creating rules. You can also use the buttons on the toolbar.

  A new line appears in the table. It has default parameters.



To manage a rule:

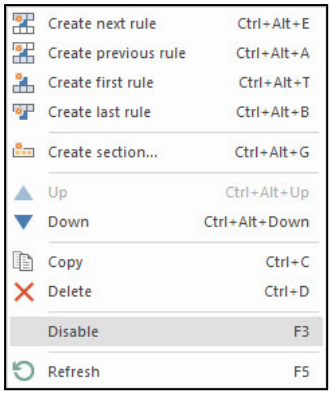
Note.
To select several rules, hold **<Shift>** or **<Ctrl>** and click the required lines.

1. To configure a rule, right-click the required parameter cell and select the respective command:

Command	Description
Select Add	Select one or several objects from the list
Edit	Edit the name or description of the rule
Properties	Parameter properties
Accept Drop	Select an action when the rule is applied
Delete	Delete parameter

Note.
When editing Firewall and NAT rules, you can quickly replace a network object with another one in multiple rules. For this procedure, see p. 89.

2. To delete a rule, select one or several rules (using **<Ctrl>** or **<Shift>**) and, on the toolbar, click **Delete**.
3. To enable/disable a rule, right-click its cell that contains a sequence number and select **Disable**.



A disabled rule has the respective icon to the right of its number.

4. To change the position of a rule in the list, select one or several rules and use to move up or to move down.
5. To combine rules into sections, select a rule to be the first in the section, click **Section** on the toolbar and, in the appeared dialog box, type the name of the section.

   A section combines all the rules up to the next group. You can collapse the list of rules in a section using to the left of the section name. To expand the list, use the same button. The toolbar contains buttons for collapsing and expanding all the rules in the list.

   You can move sections in the list as well as the rules. To rename a section, right-click it and select **Rename**.
6. After all the parameters are configured, save changes in the Security Management Server configuration and install the policy on the required Security Gateways (see p. **84**).

Note.
You can export the list of filtering rules with configured parameters into a file to view it later in html format. To do so, click **Export** on the toolbar, then specify the file name and saving path.

Protocol and application control

While filtering, the Firewall provides step-by-step traffic processing. After checking IP addresses, ports and protocols, you can also analyze traffic using application and protocol control.

Note.
Protocol and application control come into play only after some packets with defined payload were accepted.

Protocol and application control operates with IPS.

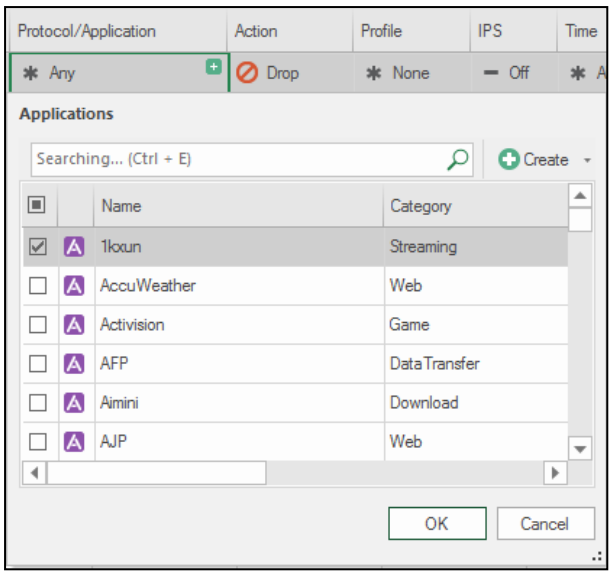
Note.
Protocol control can be used only for TCP and UDP traffic. You can set any destination port for a service. It allows you to detect a protocol that uses non-standard ports.

To use protocol and application control in a Firewall rule:

1. In the Configuration Manager, go to **Access control** | **Firewall**.
2. Select an appropriate Firewall rule or create one (see p. **34**).

   Attention!
   Protocol and application control cannot be combined with WEB/FTP filtering.
3. Move the pointer over the **Protocol/Application** cell, click .

   The list of the applications appears as in the figure below.



4. Select the required applications or application groups in the list (see p. **21**).
5. To create a protocol or application group, click **Create**.

   The **Group** dialog box appears.
6. Create a protocol or application group (see p. **31**).
7. As you select all the required objects, click **OK**.

   The selected protocols or applications and groups will be added to the filtering rule. The **Profile** field becomes unavailable for editing.

Attention!

Some web resources use security mechanism to protect from HTTPS inspection, for example, use a security protocol different from SSL/TLS. For instance, Google services use the QUIC protocol. In this case, it is required to create a Firewall rule restricting outbound traffic via UDP with destination port 443. As a result, browsers ignore the QUIC protocol and use SSL/TLS for connection.

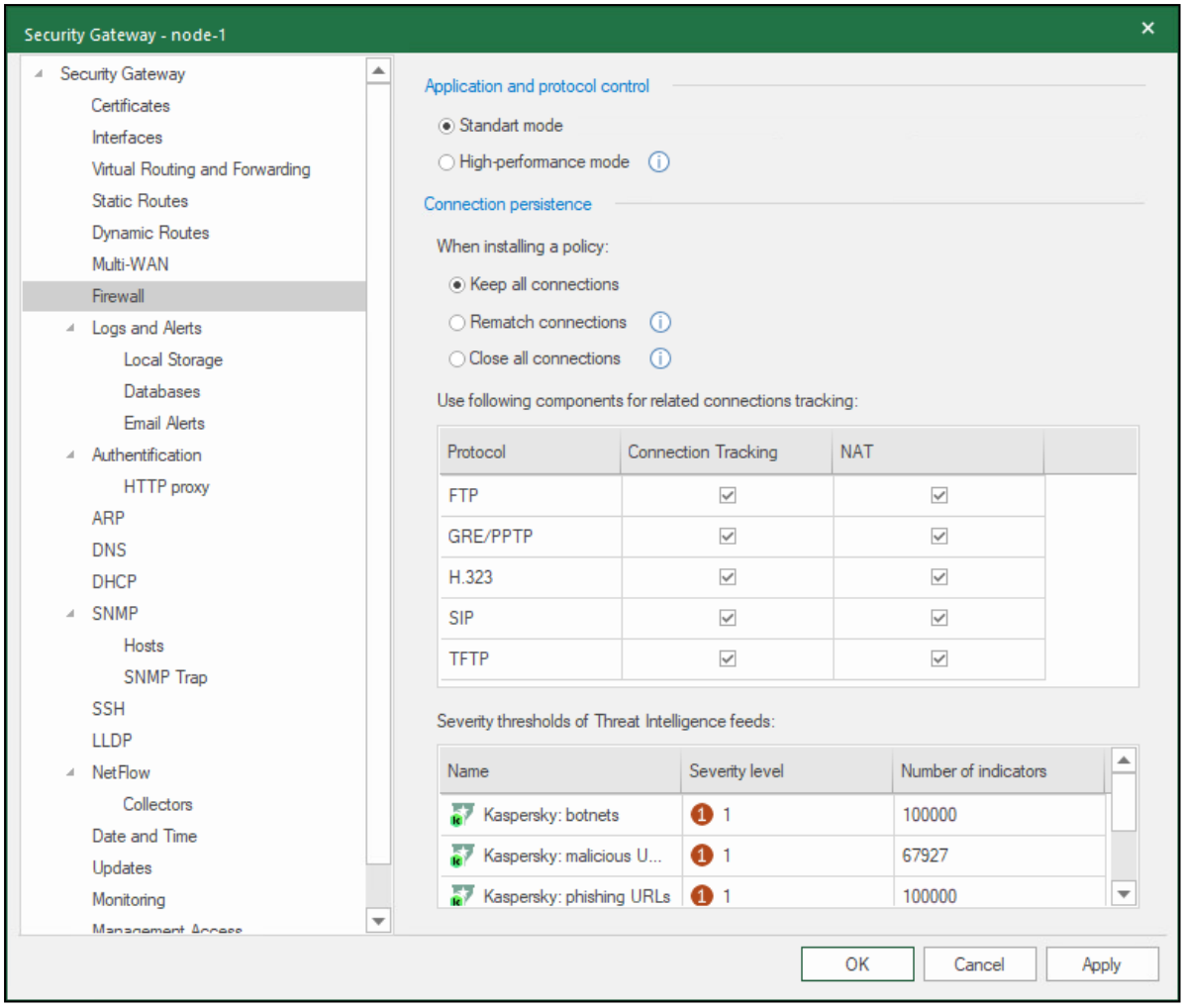
Configure the high performance mode

The protocol/application control mechanism can operate in standard mode or high performance mode. In some cases, the high performance mode can achieve faster packet processing compared to the standard mode.

By default, the protocol/application control operates in standard mode. If the packet processing does not become faster after you switch to the high performance mode, switch it back to the standard mode.

To switch to the high performance mode:

1. Open the properties of the Security Gateway for which you need to enable the high performance mode of protocol/application control.
2. In **Security Gateway**, select **Firewall**.



3. On the right, in the **Application and protocol control** section, select **High-performance mode**.
4. Click **OK**.

   The dialog box closes.
5. Install the policy on the Security Gateway.

Advanced application control

Advanced application control enables more detailed traffic filtering than basic application control (see p. **35**). This mode allows you to use an enhanced and updated list of applications. Each application has its own set of attributes. Traffic can be filtered using these attributes.

You can create a copy of an application with a custom set of parameters and attributes. It enables more detailed filtering.

Applications can be combined in groups to be used as rule parameters. A group can be included into another group (parent) and, thus, create a hierarchy.

The advanced application control files are included in an update packet that can be downloaded to the Security Management Server from the Update server or uploaded manually.

To perform the updating, the required Security Gateway and the Security Management Server must have at least one license for the component. To access the enhanced list of applications in the Configuration Manager, update the Security Management Server.

After the license expires, advanced application control is still in operation but the application list cannot be updated.

By default, basic application control is enabled on all the Security Gateways.

Attention!
You cannot use basic and advanced application control simultaneously on the same Security Gateway.

List of protocols/applications

Applications downloaded to the Security Management Server database are displayed in the list of Security Management Server objects. The list also contains applications for basic control.

To view a list of applications:

- In the **Objects** area (see p. **12**), select **Protocols and Applications**.

  In the list, protocols and applications of basic and advanced control are distinguished by their icons:

  — basic control application or protocol;

  — basic control protocol for a high performance Firewall;

  — advanced control protocol;

  — advanced control application.

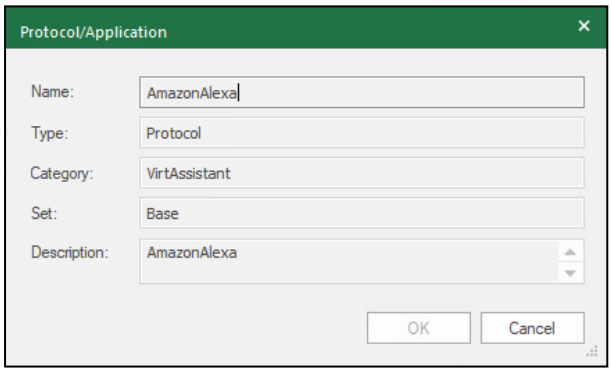
To view protocol/application data:

- Right-click the required protocol/application and select **Properties**.

  Note.
  To view applications of basic or advanced control separately, use a filter. To search for the required application, use the search box.

  The **Protocol/Application** dialog box appears. The dialog box may differ depending on types of protocols and applications.

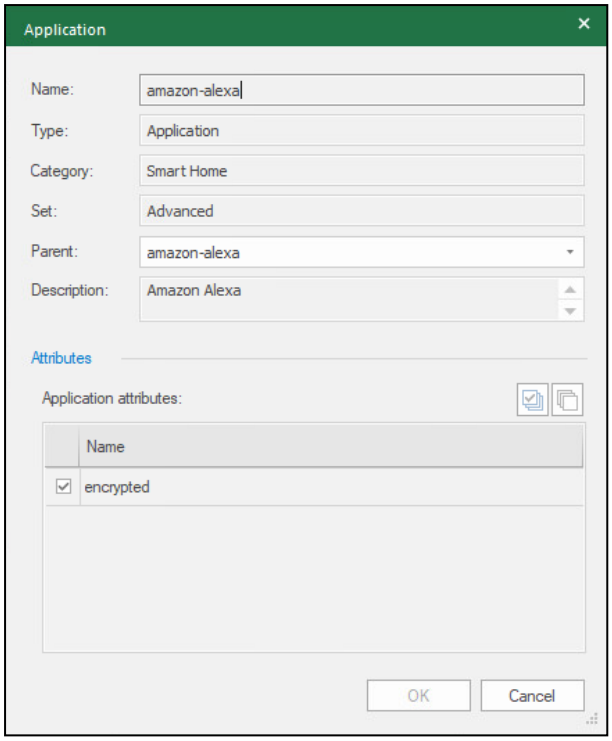
  You can see the dialog box for basic protocols and applications in the figure below.



  General information about a protocol or application includes:

  - name;
  - type (protocol or application);
  - category;
  - set (base or advanced);
  - description.

  You can see the dialog box for advanced protocols and applications in the figure below.



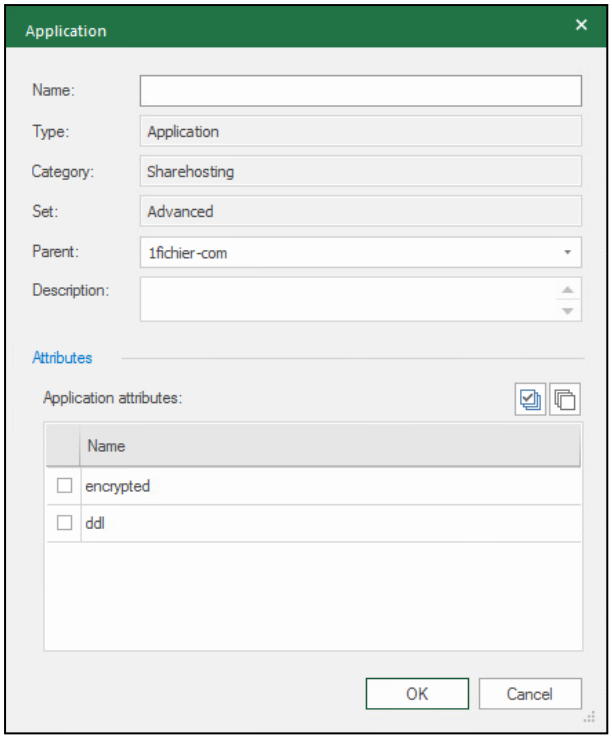
The dialog box contains the following data:

- name;
- type;
- category;
- set;
- parent;
- description;
- set of attributes.

Create a new application

To create a new application:

1. In the list of applications (see p. **38**), right-click an application to be copied and click **Create Application**. The **Application** dialog box appears.



The **Type** and **Category** parameters contain data respectively to the selected application.

Note.
To create a copy of an application, in the **Type** drop-down list, select the required application. The **Category** parameter changes respectively.

2. Enter a name for the new application and its brief description.

Attention!
The name of a new application must be different from the original one.

3. In the **Attributes** section, select the required attributes for filtering.

   To select/clear all the attributes, use the respective buttons .

4. After you configure the attributes, click **OK**.

   The **Application** dialog box closes. The created application appears in the list.

5. After all the parameters are configured, save changes in the Security Management Server configuration.

Application groups

For detailed information about creating the groups, see p. **31**. You can also select an application or a group in the list, right-click the required object and click **Create group**. In this case, the selected application/group is already included in the new group.

The created groups are displayed at the bottom of the list. You can perform standard operations (deleting, viewing and editing) for these groups.

Configure Firewall rules

Go to the list of Firewall rules and select the required rule or create a new one. Add the required applications/groups of applications to the rule.

Attention!
Drop rules for applications must be located higher than **Accept** rules for traffic.

Protocol inspection in services can use protocols from Advanced application control.

Applications from the Advanced application control list are sorted by categories that can be used in rules.

To save the rule reaction to the network security log, select the respective parameter in the **Log** cell.

Select the Security Gateways for this rule. The **Advanced application control** component must be enabled on these Security Gateways.

Save the changes and install the policy on Security Gateways used in the Firewall rule.

You can view events of the advanced application control rule action in the network security log (see [**3**]).

You can configure advanced application control rules more precisely by blocking a specific type of application traffic. You can set a specific type of application traffic by selecting certain application attributes.

To configure a rule more precisely:

1. Go to the list of **Firewall** rules and create a new rule.
2. In **Application** cell, click and click **Create** in the drop-down list.
   The **Application** dialog box appears.
3. In the **Type** cell, select an existing application as a template to create a new one.
4. In **Application** attributes, select the attributes by which the rule is required to be checked.
5. Enter a name and a short description of the new application and click **OK**.
   The **Application** dialog box is closed.
6. Configure other parameters of the **Firewall** rule.

Note.
You can edit a set of used attributes for the newly created application later if necessary.

Team Viewer limitations

If there is an open session of Team Viewer at the moment of applying a policy with a rule for Team Viewer, the rule does not work after the policy is applied. The rule will work only after closing the current session and attempting to create a new one.

WEB/FTP filtering

The Firewall optionally enables the advanced filtration mechanism which allows you to analyze and process transit network traffic on the level of some protocols. These protocols are:

- HTTP;
- HTTPS;
- FTP.

The mechanism works as a proxy, performs a man-in-the-middle attack by posing as the requested web resource for the request source and establishes a connection to the web resource on its own behalf. If **HTTPS** is in use for communication with a web resource, then this mechanism performs an HTTPS inspection (traffic decryption) with certificate substitution.

Filtering is provided using Firewall rules. WEB/FTP profiles are used to add filtering mechanism to Firewall rules. A profile contains a set of filters that includes both actions to be performed when using each filter and redirection address if necessary.

The following objects may be considered as WEB/FTP filters:

- pre-installed Kaspersky filters for malicious URL blocking;
- pre-installed Security Code filters;
- pre-installed URL filters by the SkyDNS categories;
- ECAP services for filtering by the hash database of Kaspersky malicious files and by the custom hash database;
- ICAP servers for traffic transmission to the external antivirus server;
- custom filters created in the Configuration Manager.

However, some web resources can use security mechanisms against HTTPS inspection, which makes it impossible to use the Web/FTP filtering mechanism as part of the Firewall. To maintain access to such web resources, you can specify a set of exceptions for HTTPS inspection (see p. **55**).

The Firewall comes with a pre-installed set of vendor exceptions. The set can be updated by the producer using the update server.

The administrator can create new exceptions and add them to this list.

Attention!
For proper WEB/FTP filtering, the DNS service should be configured on a Security Gateway (more on DNS configuration, see in [**5**]).

Configure WEB/FTP filtering

To configure WEB/FTP filtering, take the following steps:

1. Initial configuration (see below).
2. Create Firewall rules which allow access to web resources.
3. Create NAT rules which allow access to web resources.
4. If necessary, create custom WEB/FTP filters and groups of filters (see p. **46**).

> **Note.**
> Filters inside a group function according to the **OR** logic.

5. Configure WEB/FTP filtering profiles for the required addressing scheme of Internet resources (see p. **51**). When you configure profiles, filter groups (both pre-installed and custom) are included in them.

> **Note.**
> Filters inside a profile function according to the **OR** logic.

6. Add the profile in the Firewall rule (see p. **55**).

> **Attention!**
> - You cannot select WEB/FTP filtering and protocol inspection or application control in a Firewall rule at the same time.
> - To enable WEB/FTP filtering for different application protocols, you need to create a separate Firewall rule, WEB/FTP filter and profile.
> - You need to select a certain service for a certain profile type in a WEB/FTP filtering rule. You cannot select **Any** or **Any TCP** in the **Service** cell because it causes other parameters of this rule to work incorrectly.
> - The rule with WEB/FTP filtering profiles must be the last in the list for this network, because after passing it traffic for this network does not return to the Firewall for processing by the next rules.
> - The Multi-WAN rules must not match the rules in which the **Malicious URL Blocking** component is enabled. In the case of source, destination and service match in the Multi-WAN rules and rules with Malicious URL Blocking, the latter will not work. You should either use exceptions in the Multi-WAN rules or avoid configuring Multi-WAN rules for the traffic that requires rules with Malicious URL Blocking processing.
> - If user groups, URL categories or Kaspersky/Security Code filters are used in Web/FTP filtering alongside ECAP/ICAP services, we recommend creating two different profiles and two respective Firewall rules. In this case, the position of a rule with ECAP/ICAP services in the Firewall rule list must be lower than the position of a rule that includes user groups/URL categories/Kaspersky/Security Code filters.

7. Install the policy on the required Security Gateways (see p. **84**).
8. Analyze the traffic flow and, if there is no access to the required web resource, add the required exception to the list.

Initial configuration

To use WEB/FTP filtering:

1. Enable the Malicious URL component in the Security Gateway properties:
   - Malicious URL Blocking (the respective license is required);
   - SkyDNS URL Blocking (the respective license is required);
   - Antivirus (the respective license is required).

> **Attention!**
> An additional license is not required to work with a group of filters.

2. In the **Security Gateway** dialog box, go to the **DNS** subsection, type the IP address of the DNS server. DNS configuration is required because the Malicious URL Blocking component intercepts a client request and initiates a new connection from the components name which requires converting names to IP addresses.
3. WEB/FTP filtering via HTTPS requires the root RSA certificate and the SSL/TLS inspection certificate to be created (see below).

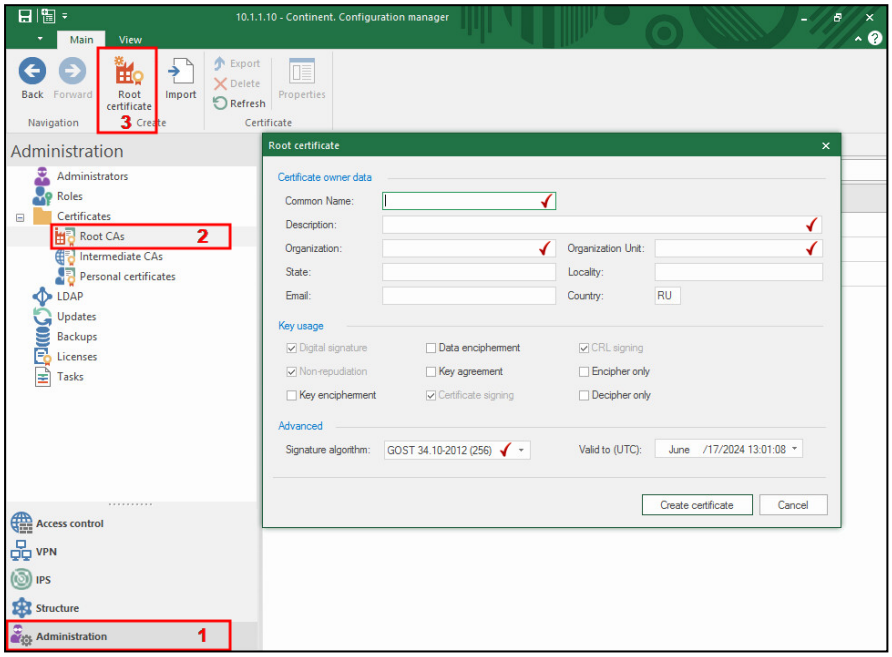
> **Attention!**
> It will suffice if you create one SSL/TLS inspection certificate, and then bind it to both devices (primary and standby).

4. Link the created certificates to the Security Gateways where you need to install firewall rules with HTTPS filtering (see p. **44**).
5. Install the policy on the Security Gateway.
6. On client workstations, install the root RSA certificate created in step **3** in the trusted certificate storage.

Creating a root certificate

To create a root certificate in the Configuration Manager:

1. In the Configuration Manager, go to **Administration** | **Certificates** | **Root CAs**.
   You can see a list of installed certificates in the display area.
2. On the toolbar, click **Root certificate**.
   The **Root certificate** dialog box appears as in the figure below.

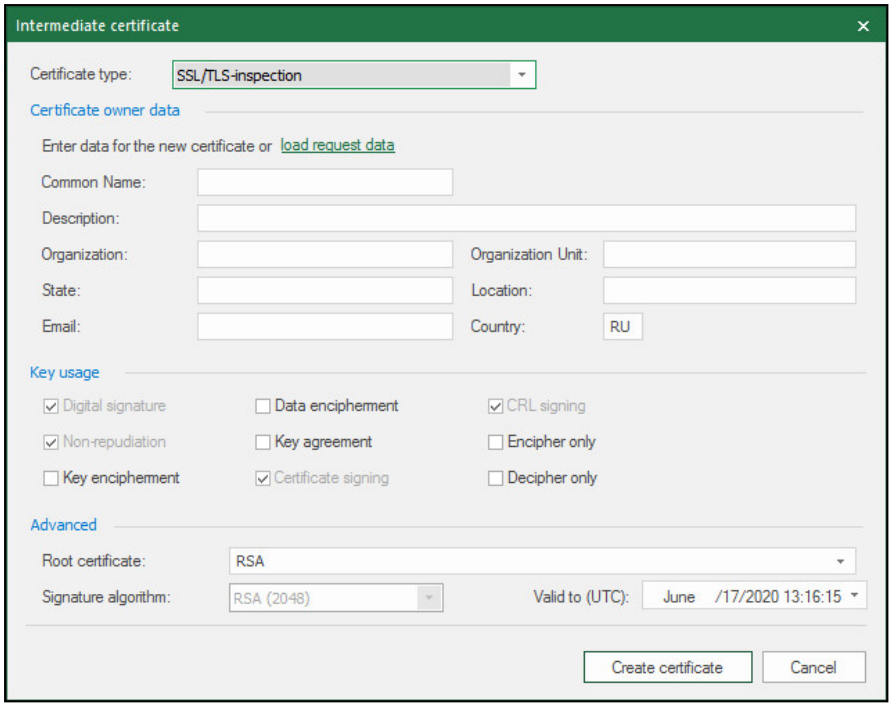


3. Specify all the required information in the **Certificate owner data**, **Key usage** and **Advanced** group boxes and click **Create certificate**.
   You are returned to the list of the root certificates where you can see the created certificate.

Create SSL/TLS inspection certificates

To create an SSL/TLS inspection certificate in the Configuration Manager:

1. In the Configuration Manager, go to **Administration | Certificates | Intermediate CAs**.
   The list of installed certificates appears in the display area.
2. On the toolbar, click **Intermediate certificate**.
   The **Intermediate certificate** dialog box appears as in the figure below.



3. In the **Certificate type** drop-down list, select **SSL/TLS-inspection**.
4. Specify all the required parameters in the **Certificate owner data** and **Key usage** sections.
5. In the **Advanced** section, select the previously created root certificate and specify an expiration date.
6. Click **Create certificate**.
   The intermediate certificate is created and its data is displayed in the list.

Link a certificate

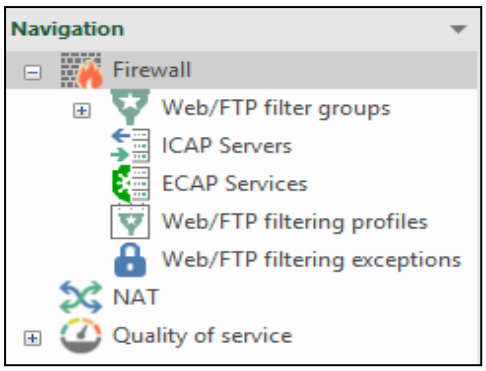
To link a certificate:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.
2. On the left, go to **Certificates**.
   The list of installed certificates appears on the right.
3. In the **Server certificates** section, click to add a new certificate.
   The **Certificate** dialog box appears.
4. Select the previously created SSL/TLS-inspection certificate in the list.
   The certificate is added to the list.
5. In the **Root certificates** section, click to add a new certificate.
   The **Certificate** dialog box appears.
6. Select the previously created root certificate and click **OK**.

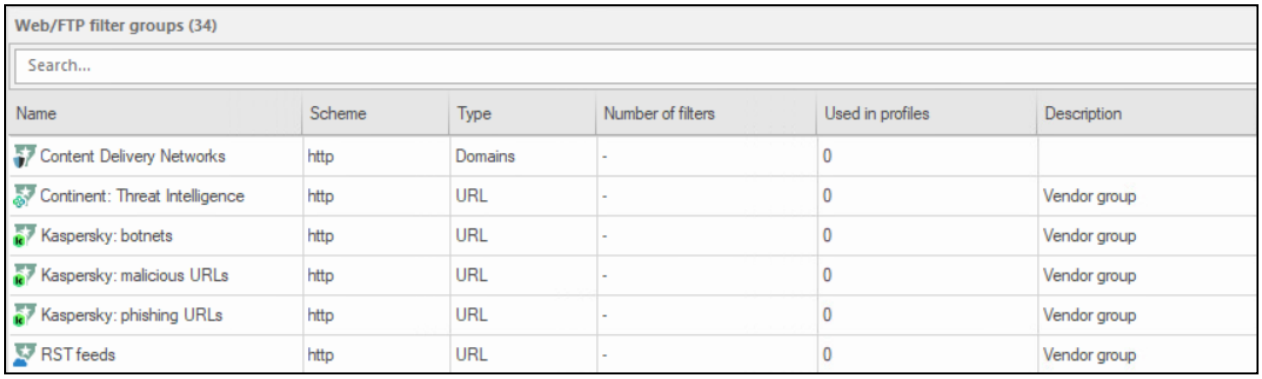
View the list of filters

To view the list and work with filters:

- in the Configuration Manager, go to **Access control | Firewall | WEB/FTP filter groups**.



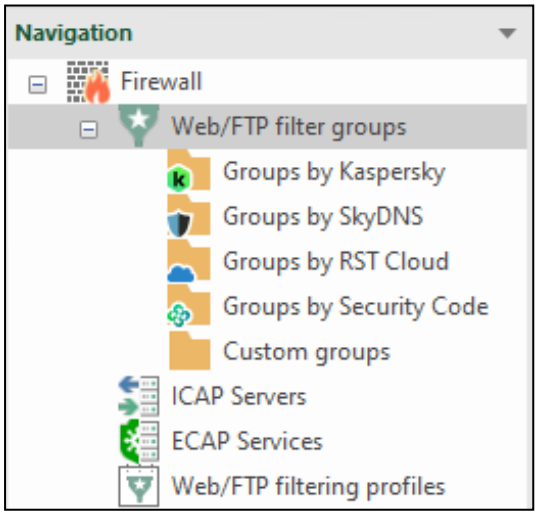
The list of the filter groups appears in the display area.



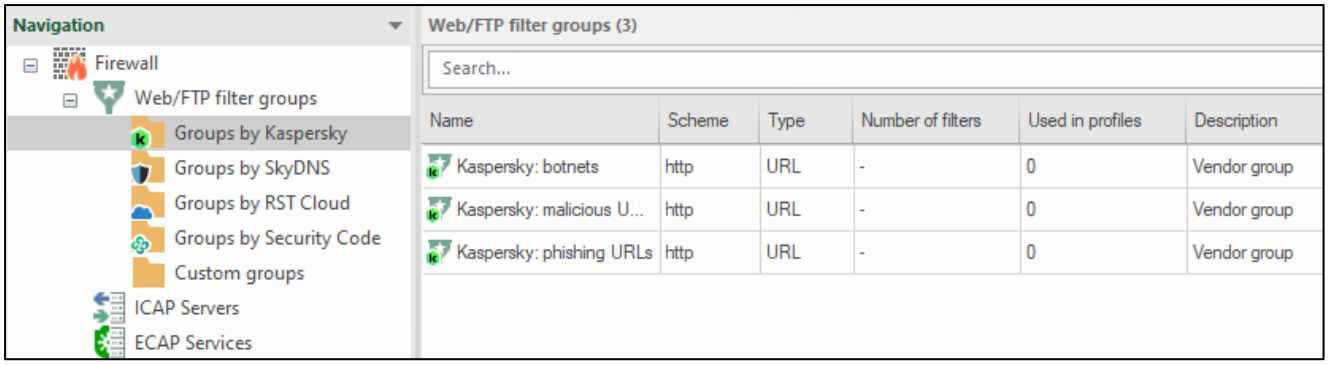
The list contains pre-installed groups of vendor rules and custom filtering groups if they were created. Custom groups are indicated by .

To view groups by categories:

1. On the navigation panel, expand **Web/FTP filter groups**.
   Folders with filter groups by categories appear.



2. Select any folder.
   You can see a list of filter groups included in this category on the right.



You can find custom filter groups in the **Custom groups** folder.

Work with custom WEB/FTP filters

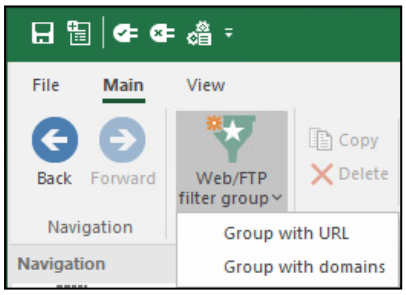
In **Web/FTP filter groups**, you can perform the following operations:

- create a new group;
- rename a group;
- delete a group;
- create a group structure (adding, deleting and editing filters).

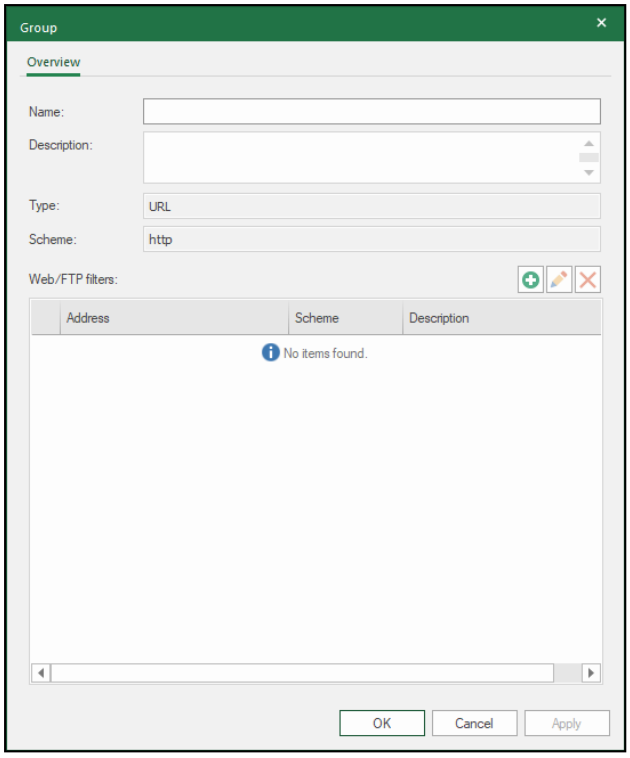
For working with pre-installed vendor filters, see other sections.

To create a new filter group:

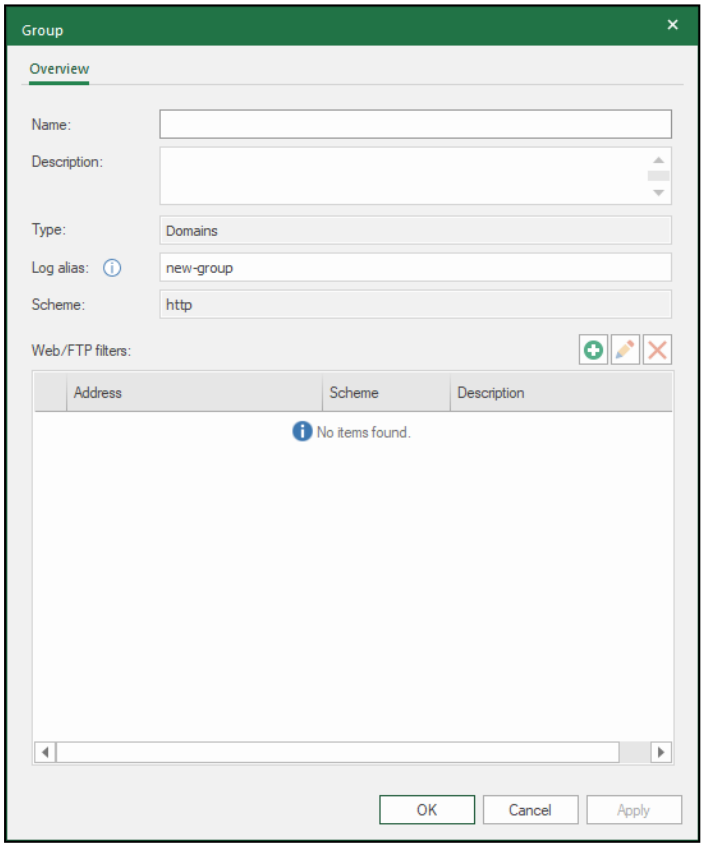
1. On the navigation panel, go to **Web/FTP filter groups** and click **Web/FTP filter group** on the toolbar.
   A shortcut menu with the following options appears:
   - **Group with URL**;
   - **Group with domains**.



2. Select the type of the created group.
   The dialog box for creating a group appears. The dialog box layout depends on the group type.
   You can see the dialog box for the group with URL in the figure below.



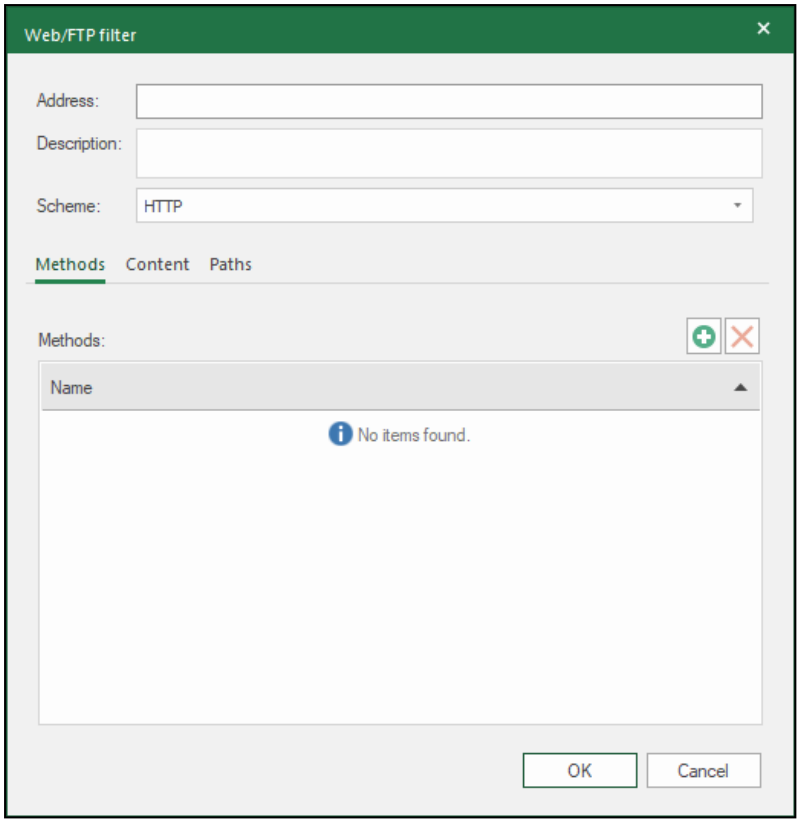
You can see the dialog box for the group with domains in the figure below.



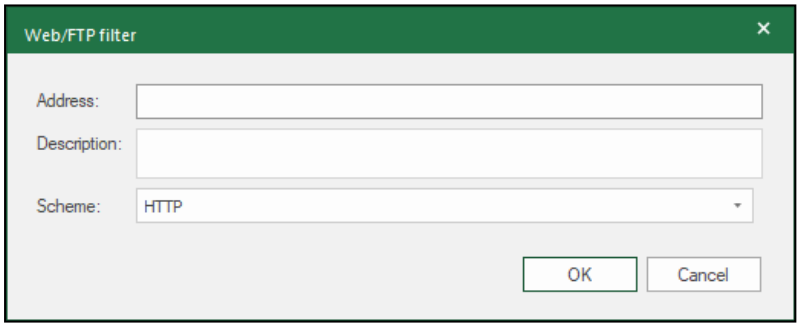
3. Enter a name and description for the group.
4. For a group with domains, specify **Log alias**. This parameter is used to identify the group during event registration in the network security log. The minimum length in characters is **1**, the maximum is **20**.
5. Add Web/FTP filters to the group. To do so, click  .

   The **WEB/FTP filter** dialog box appears. The dialog box layout depends on the filter type.

   You can see the dialog box for the **URL** type in the figure below.



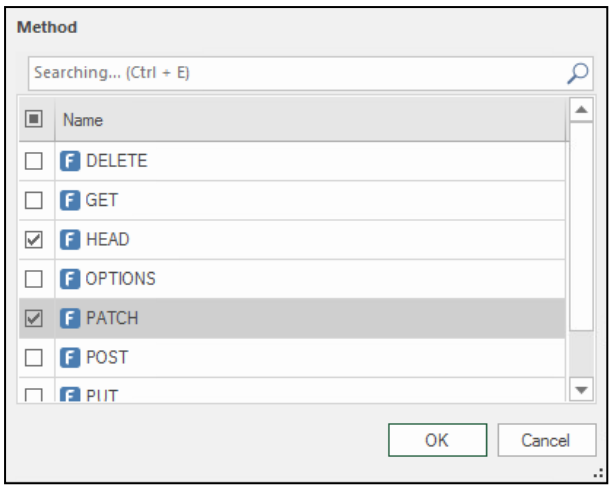
You can see the dialog box for the **Domains** type in the figure below.



6. Specify all the required WEB/FTP filter parameters:

Parameter	Description
Address	Domain name of a server. URL that will be specified in the **Address** field implies searching by a solid URL. Regular expressions are case-sensitive. You can leave the field empty or to use the syntax of regular expressions, for example, a point. In this case, the match on the **Paths** tab will be applied to all URLs as a point is a metacharacter that complies with every character but the newline character
Description	Short description of a filter in any form
Scheme	Addressing scheme. To filter under the HTTPS protocol, create an RSA root certificate in the Configuration Manager and certificates of SSL/TLS inspection

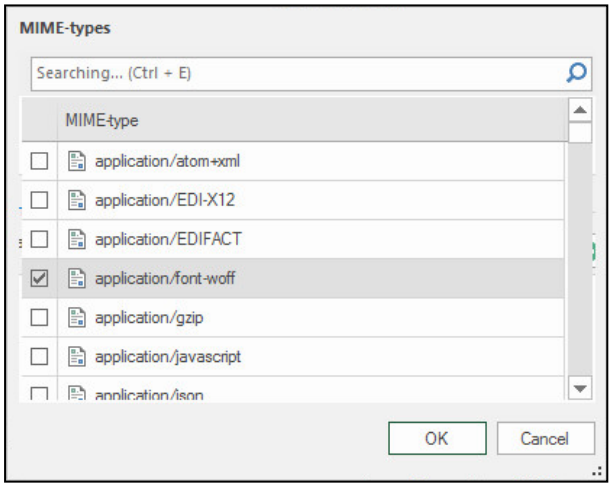
7. On the **Methods** tab, specify a data request method. To do so, click , select the methods and click **OK**. Multiple choice is available using **<Ctrl>**/**<Shift>** and **<Space>**.



Note.
The filter parameters are applied via the **AND** logical operator. If you select several objects in a single parameter, the selected parameters are applied via the **OR** logical operator.

Attention!
If a group contains at least one filter, all other filters will be created with the same addressing scheme.

8. On the **Content** tab, create a list of required data types:
   - to add new data types to the list, click and select the required MIME types. Then click **OK**. Multiple choice is available using **<Ctrl>**/**<Shift>** and **<Space>**.



   - to delete an object from the list, select the MIME type and click .
9. If necessary, specify the respective file extensions by which filtering is performed. Examples of such extensions:

Description	Example
By one extension	exe
By several extensions	exe,zip,jpg
	exe, zip, jpg
	.exe, .zip, .jpg

10. On the **Paths** tab, enter web-pages names, uploaded files names, or respective regular expressions:
    - to add a new element to the list, click , then type the required expression in the appeared text box;
    - to delete an element from the list, select the required one and click ;
    - to edit element's parameters, select the required one in the list and click .
11. After you configure all the required parameters, click **OK**.

The **WEB/FTP filter** dialog box closes and you can see the created filter in the list.

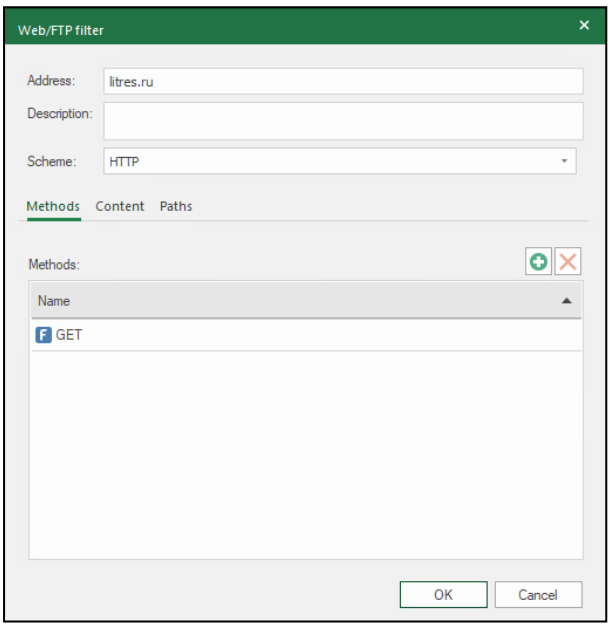
Paths

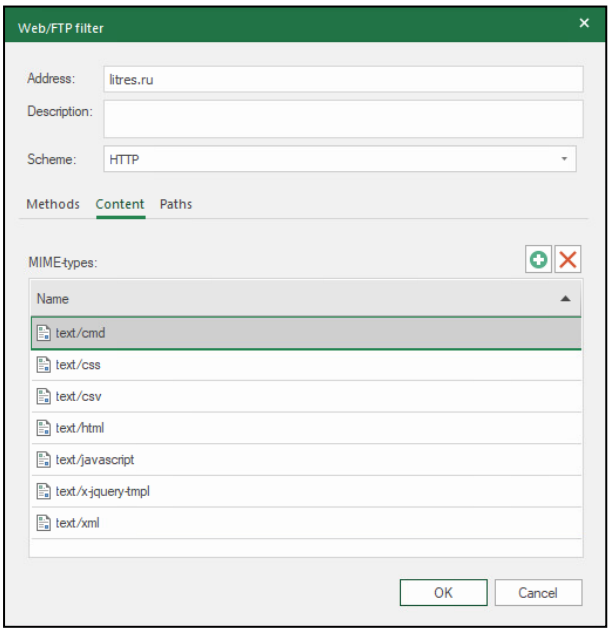
You can use regular expressions while configuring the paths in filter properties. They enable an additional feature that defines whether the firewall rule should be applied to IP packets. This feature is a special information object or attribute within the IP packet data field.

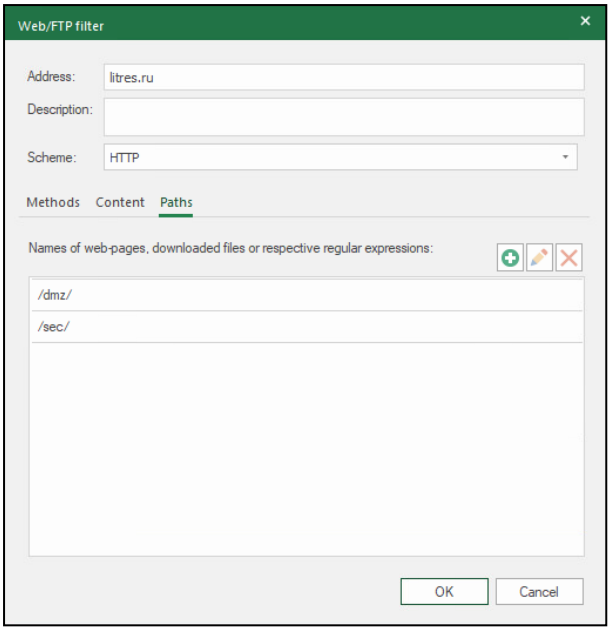
A regular expression also contains a configured way to detect the attribute or information object within the transmitted packet data field. The mechanism uses the common rules of using the metacharacters in the regular expressions. For detailed information about the metacharacters.

You can use several regular expressions in one filter. If one of the expressions is detected, the rule is applied with the respective reaction.

For example, to enable access control via HTTP there is a filter that uses the GET method and the regular expressions as in the figures below.







As a result of using this filter, the **HTML** or **XML** files from the **dmz** or **sec** folders of the **litres.ru** HTTP server will be filtered.

To delete a filter from a group:

1. On the navigation panel, select the required filter group.
   The list of filters that belong to the selected group appears in the display area.
2. Select the required filter and, on the toolbar, click **Delete**.
   The dialog box prompting you to confirm the procedure appears.
3. Click **Yes**.
   The filter is deleted from the group.

To edit filter parameters:

1. Select the required filter and, on the toolbar, click **Properties**.
   The **WEB/FTP filter** dialog box appears.
2. Modify the required parameters (see p. **47**) and click **OK**.
3. Save changes in the Security Management Server configuration.

To rename/delete a group:

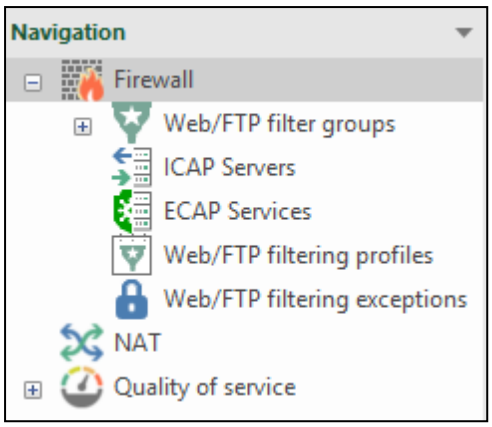
- On the navigation panel, go to **Web/FTP filter groups**, right-click the required group and select the respective command.

WEB/FTP filtering profile

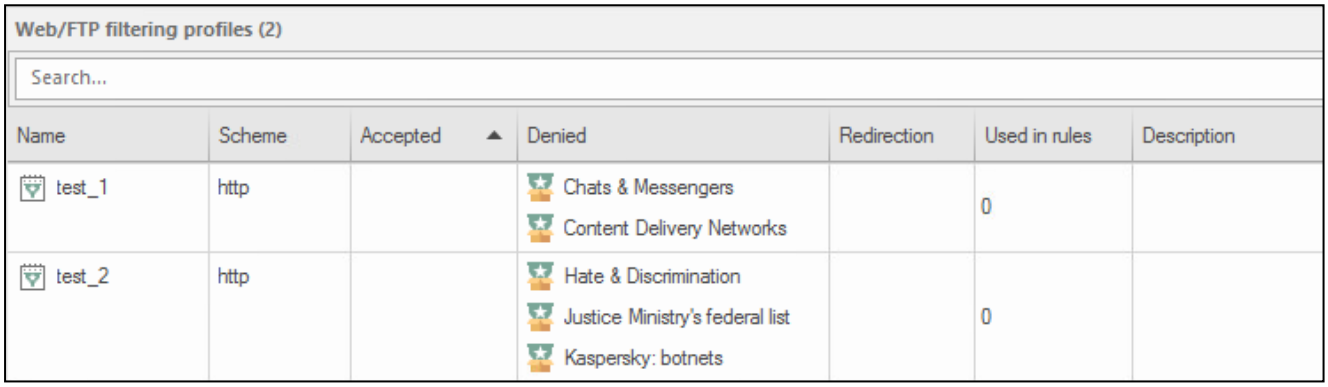
Profiles are used to include Web/FTP filters to Firewall rules specifying actions when activated.

To view a list of profiles and operate with them:

- in the Configuration Manager, go to **Access control | Firewall | WEB/FTP filtering profiles**.



The list of profiles appears in the display area.



Note.
If profiles were not created, the list is empty.

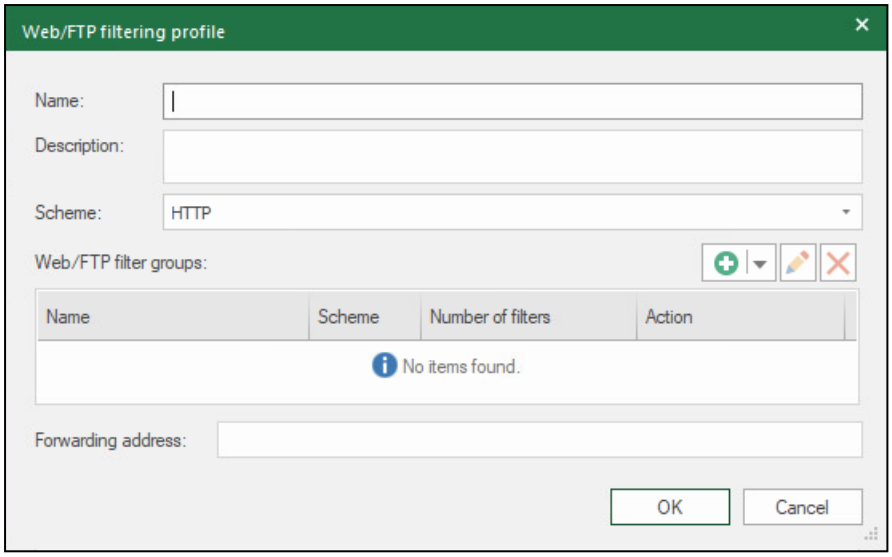
The following parameters are provided for each profile during its creation:

- **Name**;
- **Scheme** (http, https, ftp);
- **Accepted** — filter group categories that have **Accept** in the **Action** parameter.
- **Denied** — filter group categories that have **Deny** in the **Action** parameter.
- **Redirection** — filter group categories that have **Redirect** in the **Action** parameter.
- **Used in rules** — the number of rules where the profile is used.
- **Description** — short profile description.

To create a profile:

1. In the Configuration Manager, go to **Access control | Firewall | WEB/FTP filtering profiles** and click **WEB/FTP filtering profile** on the toolbar.

   The **Web/FTP filtering profile** dialog box appears.

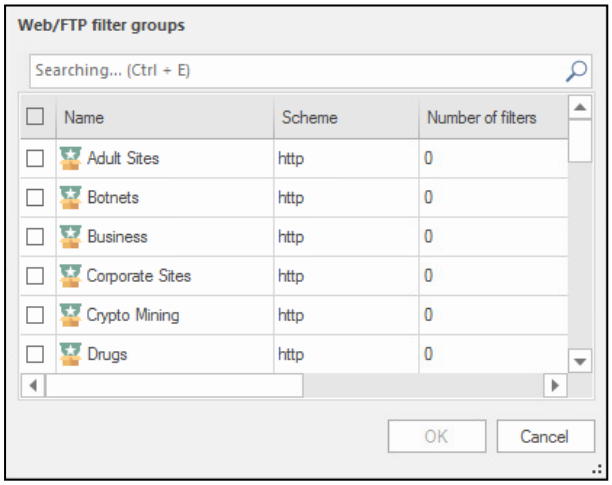


2. Specify all the required WEB/FTP filtering profile parameters:

Parameter	Description
Name	Name of a profile
Description	Short description of a profile in any form
Scheme	Addressing scheme: FTP, HTTP or HTTPS. To filter under the HTTPS protocol, create a root RSA and SSL/TLS inspection certificates. In profiles with FTP scheme, you can use only custom filtering groups. When choosing an HTTPS scheme, it is available to add elements for both HTTP and HTTPS scheme

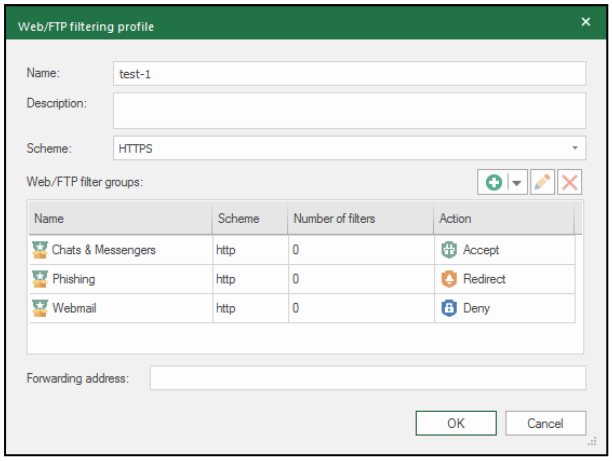
3. Add Web/FTP filter groups to the profile. To do so, click  .

   The **Web/FTP filter groups** list appears.



4. Select the required groups and click **OK**. You can select several groups by using **<Ctrl>**/**<Shift>** and pressing **<Space>**.

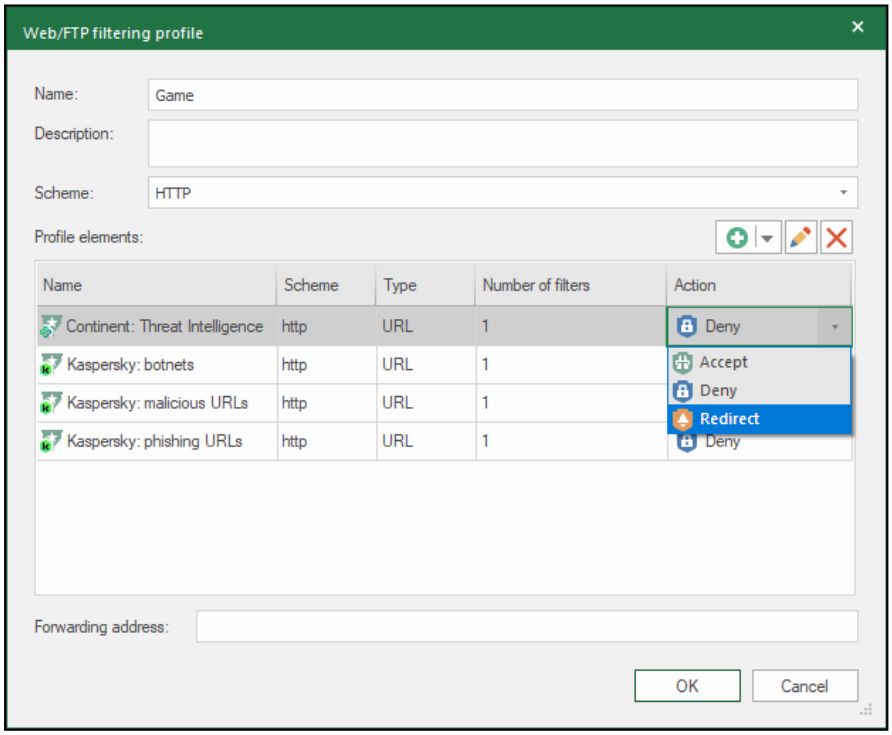
   The selected groups will be included in the profile.



5. To add ICAP servers and/or ECAP services to a profile, click .
6. In the list, select the required type of an element.
7. Adding ICAP servers and/or ECAP services is performed similarly to WEB/FTP filters.
8. In the **WEB/FTP filter groups** table, specify an action for each group in the system:

Action	Description
	Accept (traffic will be accepted)
	Deny (traffic will be blocked)
	Redirect (traffic will be redirected to a server specified below)

To do so, in the **Action** drop-down list, select the required parameter.



9. If **Redirect** is selected, specify the **Forwarding address** parameter where all the respective packets will be redirected, for example **http://address**.
10. Click **OK**.

    The profile is created and added to the list.

To create a copy of a profile:

1. In the Configuration Manager, go to **Access control** | **Firewall** | **WEB/FTP filtering profiles**, select the required profile and click **Copy** on the toolbar.

   The **WEB/FTP filtering profile** dialog box appears with the respective parameters.
2. Modify the required parameters, then click **OK**.

   A new profile is added to the list.

To delete a profile:

1. In the Configuration Manager, go to **Access control** | **Firewall** | **WEB/FTP filtering profiles**, select the required profile and click **Delete** on the toolbar.

   The dialog box prompting you to confirm the action appears.
2. In the appeared dialog box, click **Yes**.

   The profile is deleted.

Add a profile to a rule

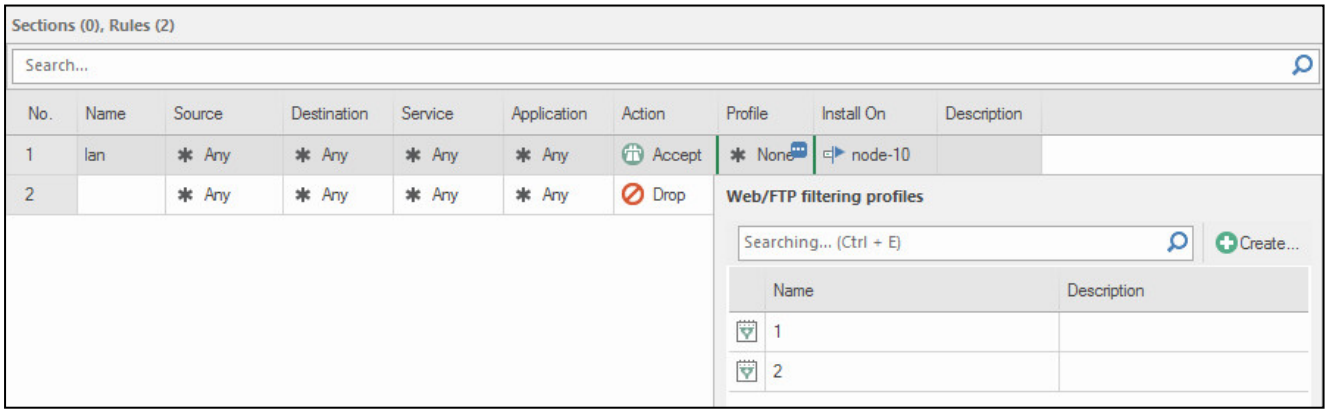
Attention!
WEB/FTP filtering cannot be combined with protocol inspection or application control in a firewall rule.

To add a profile to a filtering rule:

1. On the navigation panel, go to **Access control** | **Firewall**, select a Firewall rule or create a new one (see p. **34**).

   Note.
   WEB/FTP filtering requires a Firewall rule with the respective service. Thus, filtering by HTTP requires the **HTTP** value in the **Service** cell. **Action** must be set to **Accept**. Only one service is specified in a rule with URL filtering profile. For example, if the tcp/443 and tcp/8443 are required, a separate rule is created for each service.
2. Add the required service to the rule.

   Note.
   If NAT and QoS rules in which source/destination is specified are added to filtering rules with a profile, these rules will not be active.
3. Move the pointer over the **Profile** cell, click  and select the required profile from the list.



   Attention!
   The selected profile scheme must match the service scheme. For example, if the Firewall rule scheme is **HTTP**, the profile scheme must also be **HTTP**.
4. After you have configured all the required parameters, save the changes in the Security Management Server configuration and install the policy on the required Security Gateways.

WEB/FTP filtering exceptions

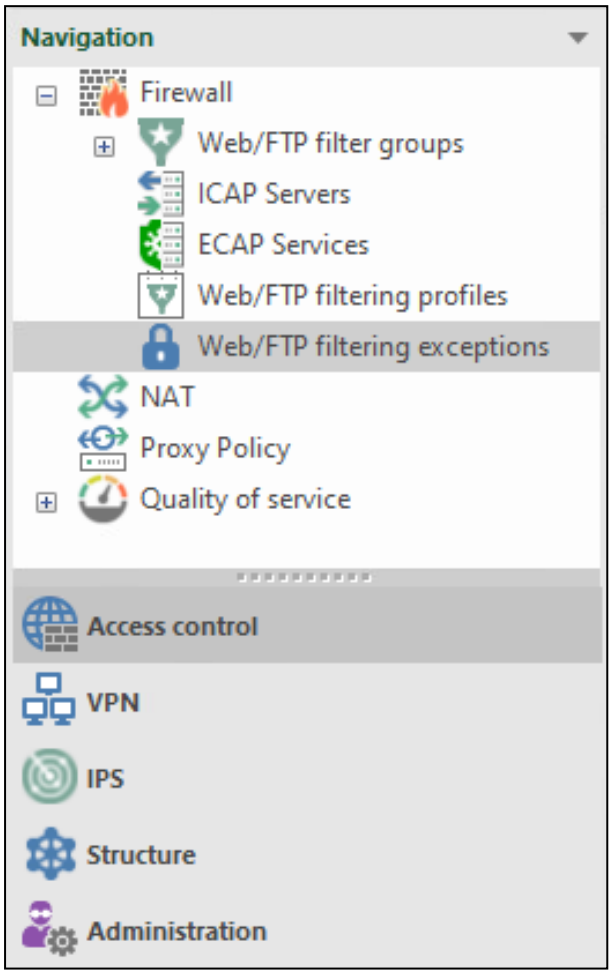
Exceptions can be used to filter HTTPS traffic. Exceptions are web resources upon accessing which the WEB/FTP filtering mechanism must not trigger.

The database of the Security Management Server contains a set of pre-configured vendor exceptions. These exceptions have the **Vendor** category. You cannot edit and delete vendor exceptions.

An administrator can add new exceptions while using Continent. When you create a new exception, it is assigned the **User** category. The **User** exceptions can be edited or deleted.

To view the list of exceptions:

- in the Configuration Manager, go to **Access control | Firewall | WEB/FTP filtering exceptions**.



The list of exceptions appears in the display area.

Every exception has the following parameters:

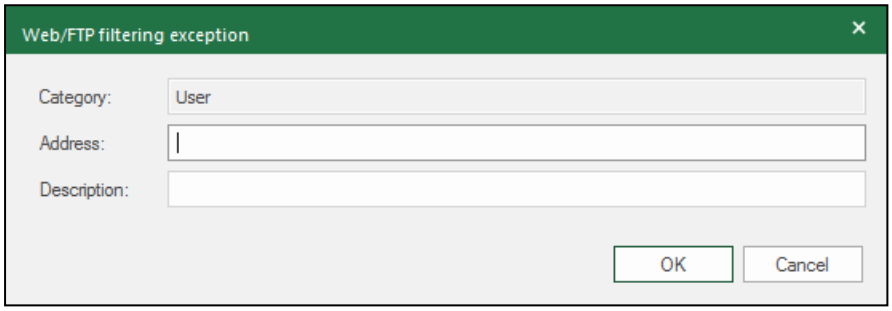
- **State** — **Enabled**/**Disabled**;
- **Category** — **Vendor**/**User**;
- **Type** — **Server name**/**Domain name**;
- **Address** — an address (name) of a server or domain;
- **Description** — a comment to an exception.

When viewing the list of exceptions, you can do the following operations:

- refresh the list of exceptions — click on the toolbar;
- sort the list of exceptions by **State** and **Category**;
- search exceptions in the list by **Address** or **Description** value;
- add a new exception;
- edit the required user exception;
- copy the required exception;
- delete the required user exception;
- change the state of the required exception.

To add a new exception:

1. Open the list of exceptions and click **Create WEB/FTP filtering exception**.
   The respective dialog box appears.



   The **User** category is assigned to the created exception.
2. In the **Address** field, specify the server or domain name. In the **Description** field, specify a short description of the exception.

   Attention!
   Exception address must not match the existing exceptions.
3. Click **OK**.
   The new exception is added to the end of the list of exceptions.

To edit an exception:

1. Select the required exception from the list and click **Properties** on the toolbar.

   Attention!
   You can edit only user exceptions.

   The respective dialog box appears.
2. Specify the new parameter values and click **OK**.
   The list displays the exception with the new parameters.

To copy an exception:

1. Select the required exception from the list and click **Copy** on the toolbar.
   The respective dialog box appears. While copying a vendor exception, **Category** changes to **User**.
2. Specify the new values of the required parameters and click **OK**.
   The list displays the exception with the new parameters.

To delete a user exception:

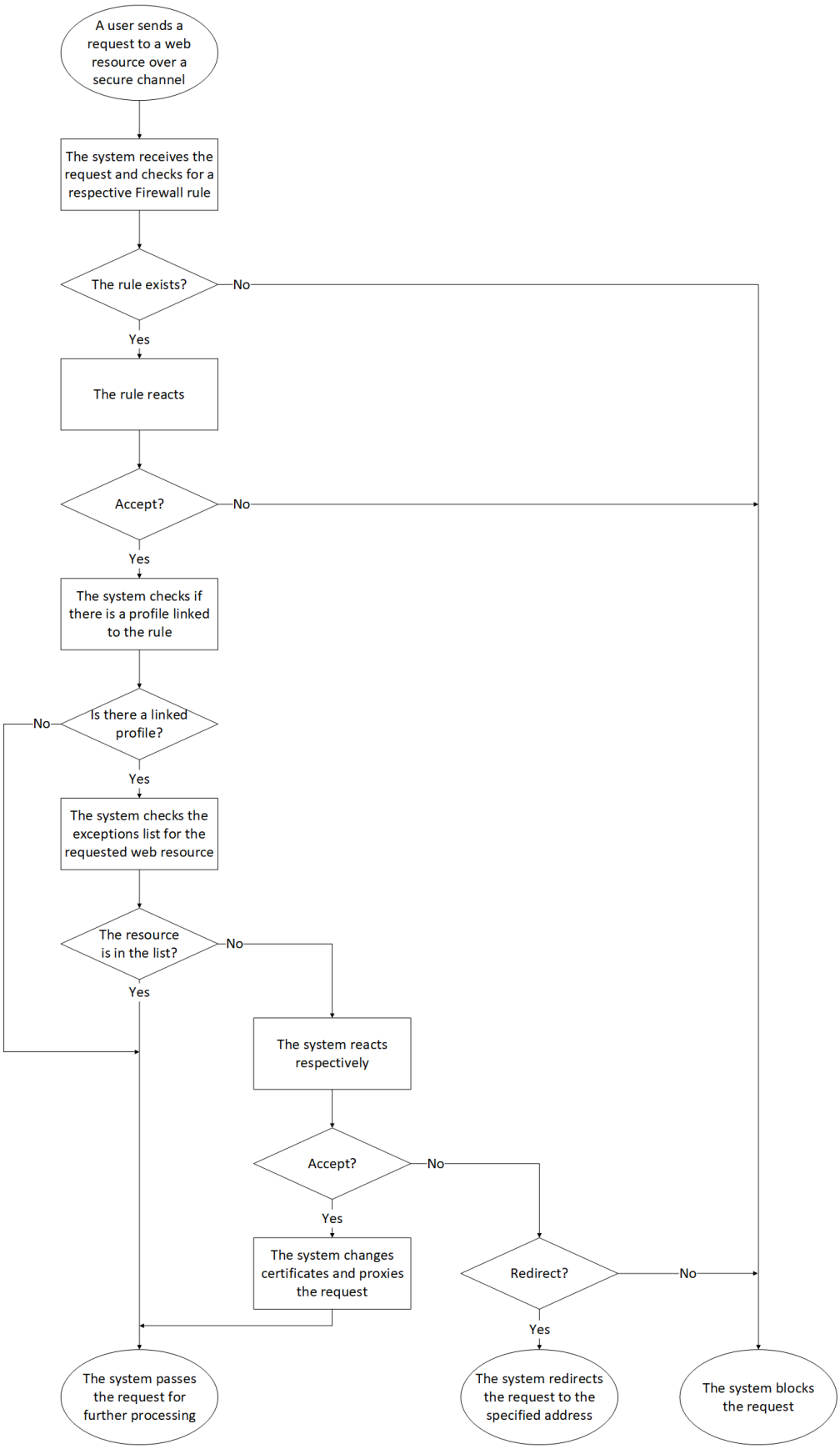
1. Select the required exception from the list and click **Delete** on the toolbar.
   The dialog box prompting you to confirm the deletion appears.
2. Click **Yes**.
   The exception is deleted from the list.

To change the exception state:

- select the required exception from the list and click **Enable** or **Disable**.
  The exception switches to the according state.

WEB/FTP filtering with specified exceptions

You can see a WEB/FTP filtering algorithm with specified exceptions below.

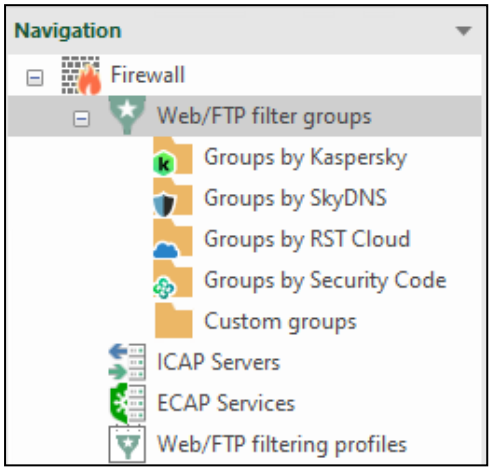


Malicious URL blocking

Continent provides a mechanism that uses a pre-installed set of filter groups provided by Kaspersky and Security Code. Filters are sets of signatures for malicious URL blocking.

To view a list of filter groups and work with them:

- In the Configuration Manager, go to **Access control | Firewall | WEB/FTP filter groups**.



Continent provides the following filter groups for protection from malicious websites:

Filter group	Threat description
Kaspersky: botnets	Botnet viruses
Kaspersky: malicious URLs	Malicious software containing viruses
Kaspersky: phishing URLs	Phishing attacks
Continent: Threat Intelligence	Malicious software, phishing attacks

Before working with Kaspersky and Security Code filters, enable malicious URL blocking on Security Gateways where the filters will be used and install updates for vendor rules (see [**6**]). Security Code filter updates are in the Kaspersky filter group.

You cannot edit or delete pre-installed groups. Their signatures are updated automatically according to the schedule configured by the administrator (see [**6**]).

To include malicious URL filters in the filtering mechanism, add them to the WEB/FTP profile and connect the profile to a Firewall rule.

Severity levels for Web/FTP filtering groups

For filter groups for protection from malicious websites, you can select which filters to use for filtering. In the filter list, vendor sets the attribute that indicates the severity level for each threat. The attribute values range from **1** to **5**, where **1** is the full list of filters. When you select any severity level value in the Security Gateway properties, all categories with higher value get in the filtering list. For example, when you select **3**, filters with categories **3**, **4**, **5** will be used. The number of filters for the selected severity level value will be displayed in a separate field.

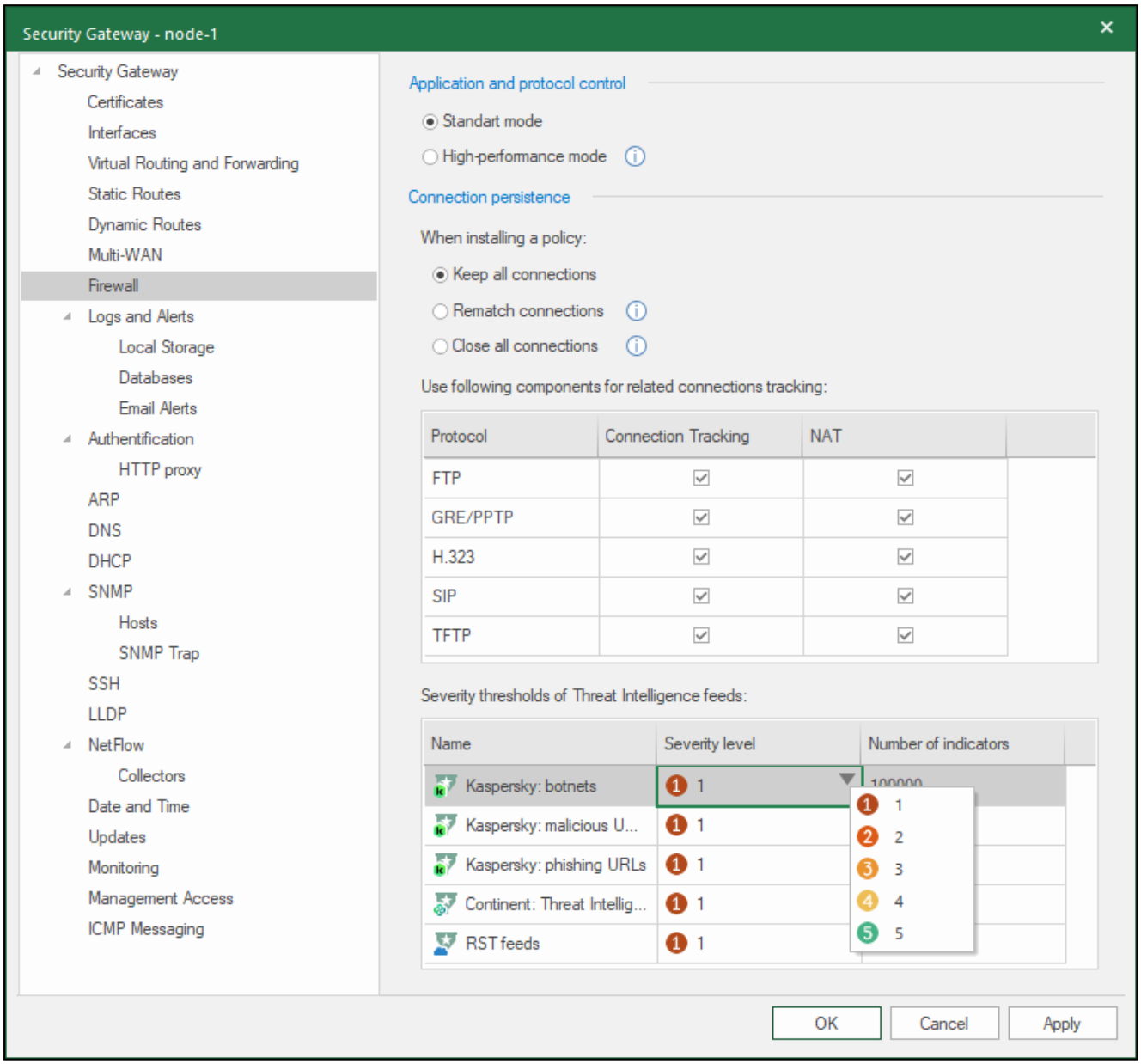
When transferring an update from the Security Management Server to the Security Gateway, the update package is transferred entirely, then a final list is generated on the Security Gateway depending on the selected severity level. The generation process starts when the policy is installed and when an update is installed. The severity level is formed for each group of filters within a single Security Gateway.

When adding a new Security Gateway or updating software, the severity level value is assigned depending on the platform family:

- SOHO — **5**;
- SMB — **3**;
- ENTERPRISE — **1**;
- Unknown — **1**.

To change the severity level for Web/FTP filtering groups:

1. Open the properties of the Security Gateway on which you need to change the severity level for Web/FTP filtering groups.
2. Go to **Security Gateway | Firewall**.
3. On the right, in **Severity thresholds of Threat Intelligence feeds**, select the required Web/FTP filtering group and expand the drop-down list.



4. Select the required severity level in the drop-down list.
5. If necessary, repeat steps **3** and **4** for other Web/FTP filtering groups.
6. Click **OK**.

   The dialog box closes.
7. Install the policy on the Security Gateway.

URL filtering by categories

Continent provides a mechanism that uses a pre-installed set of SkyDNS filter groups for URL filtering by categories.

Attention!
After Continent deployment, the Security Management Server database contains a basic set of categories. We recommend updating categories before using them in filtering rules (see [**6**], **Update vendor rules**). Update is unavailable if using a demo license.

To view a list of SkyDNS filters and operate with them:

- In the Configuration Manager, go to **Access control | Firewall | WEB/FTP filter groups**.

You cannot edit or delete pre-installed groups. Their signatures are updated automatically according to the schedule configured by the administrator (see [**6**], **Software update**).

Enable the **SkyDNS Blocking** component in the Security Gateway properties to use SkyDNS categories.

To enable URL filtering by categories, add a SkyDNS category to a WEB/FTP filtering profile and connect the profile to a Firewall rule.

The respective license is required to provide this mechanism operation.

URL filtering without SSL/TLS decryption

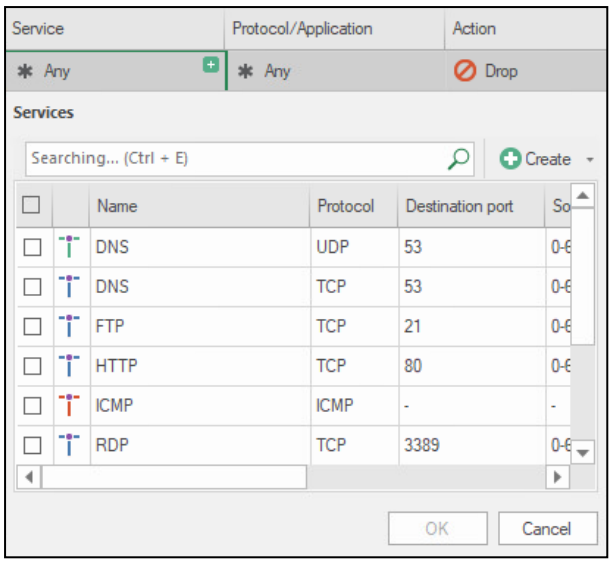
Filtering rules allow inspecting SSL/TLS traffic without its decryption. For this purpose, URL categories are used in the filtering rule. Additionally, protocols or applications from the Base control set or from the Advanced control set can be specified in the same rule.

The following requirements must be met to configure the rule on the Security Gateway:

- enable the **Malicious URL Blocking** component (a license is required for this component to work);
- there must be at least one DNS server address in the DNS settings;
- enable the **Advanced Protocols and Applications Control** component if you want to use protocols or applications from the Advanced control list (a license is required for this component to work).

To configure the rule:

1. In the Configuration Manager, go to **Access control** | **Firewall**. Select the required rule or create a new one.
2. In the **Service** field, click the hidden button .
   The list of services appears.



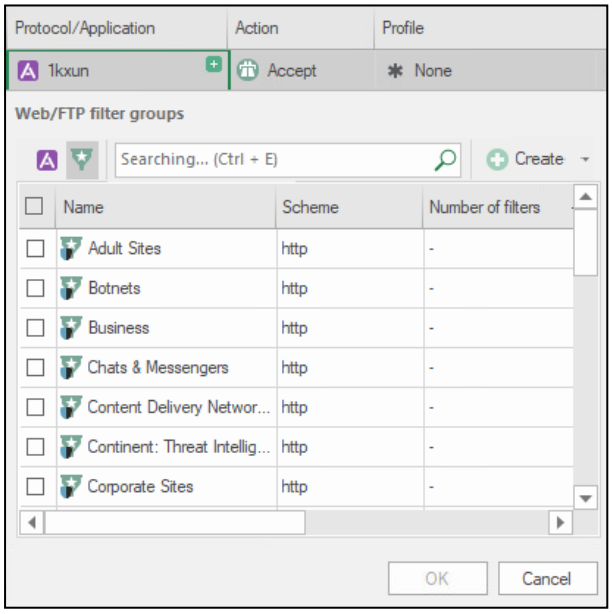
3. Select the **DNS** (port 53) and **TLS** (port 443) check boxes for services and click **OK**.

Note.
You can use the search bar to select a service (and then a category).

The selected services will be added into the **Service** field of the filtering rule.

4. In the **Protocol/Application** field, click the hidden button .
The list of base applications appears (see the figure on p. **36**).

5. Click .
The **WEB/FTP filter groups** list appears.

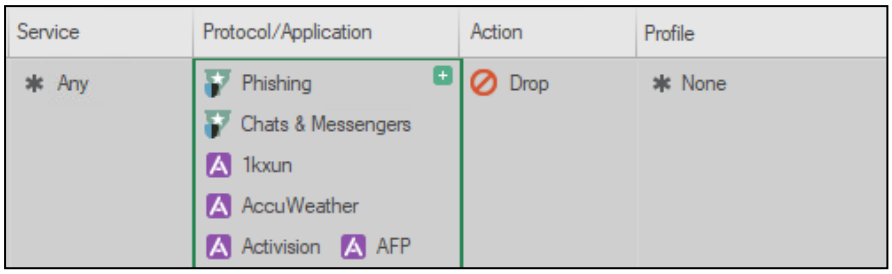


6. Select the required filter groups and click **OK**.
The selected groups will be added into the **Protocol/Application** field and the **WEB/FTP filter groups** list closes.

7. If you want to additionally add protocols/applications from the Base set or from the Advanced set to the **Protocol/Application** field, click the hidden button .
The window with the list of base set of applications appears.
Click tho following buttons to open the required list:
— to open the list of base control applications;
— to open the list of advanced control applications.

8. Select the check boxes of the required applications and click **OK**.

   The selected applications will be added into the **Protocol/Application** field and the window with the list of applications closes.



9. Finish the configuration of other filtering rule parameters and save the changes.

Configure the antivirus

The **Antivirus** component is provided by configuring ECAP services.

You can add services to WEB/FTP filtering profiles for checking traffic by malicious file hash. In this case, traffic copy is processed by the ECAP service and the result is returned to the Security Gateway that blocks or sends traffic further.

Traffic is checked using pre-installed Kaspersky and custom hashes. The administrator creates custom hashes.

To configure the antivirus operation, take the following steps:

1. The administrator creates custom hashes in the format of a **JSON** file with a specific structure, then uploads this file to the Security Management Server (see below).
2. The administrator enables the **Antivirus** component on the Security Gateways (see p. **64**).
3. The administrator uploads information about custom hashes to the Security Gateways with the enabled **Antivirus** component using the update planner mechanism (see p. **64**).
4. The administrator configures the ECAP service to use custom hashes when scanning files by the antivirus module (see p. **66**).

Attention!

After the Continent deployment, the Security Management Server Database contains a basic antivirus component. We recommend updating databases before using the antivirus in Firewall rules (see [**1**], **Update vendor rules**). Update is unavailable when using a demo license.

The antivirus operates only over HTTP/HTTPS protocols.

To enable the ECAP service mechanism, enable the **Antivirus** component in the Security Gateway properties.

An additional license is required for the **Antivirus** component to operate.

Create a custom hash file

The administrator can create a ***.json** file in any appropriate editor.

The file contains a list of records. Each record corresponds to a certain hash and contains 3 attributes:

- **md5** — 32 HEX symbols;
- **name** — 256 ASCII symbols;
- **size** — from 1 to 5242880 bytes.

Below you can see an example of a file with two custom hashes.

```
[
{
"md5": "AAD4AF9090485E80DE17A00D63216295",
"name": "Virus.MSExcel.Agent.c",
"size": 104960,
},
{
"md5": "CD4618CD64058D7D257E6FFE37432D35",
"name": "HEUR:Trojan.Win32.Generic",
"size": 61495,
}
]
```

After creating a file with custom hashes, you need to upload it to the Security Management Server repository.

To upload a custom hash file to the repository:

1. In the Configuration Manager, go to **Administration** and select **Updates**.

   You can see a list of Security Gateways with their installed updates and the contents of the update repository in the display area.
2. On the toolbar, click **Import**.

   File Explorer appears.
3. Select the ***.json** file with the custom hashes created earlier and click **Open**.

   The file upload to the Security Management Server repository starts.

   Wait for the upload to complete. After the successful upload to the repository, the imported file is displayed as an update with the following information:
   - update version;
   - type (custom hashes);
   - release date (the current time);
   - file size.

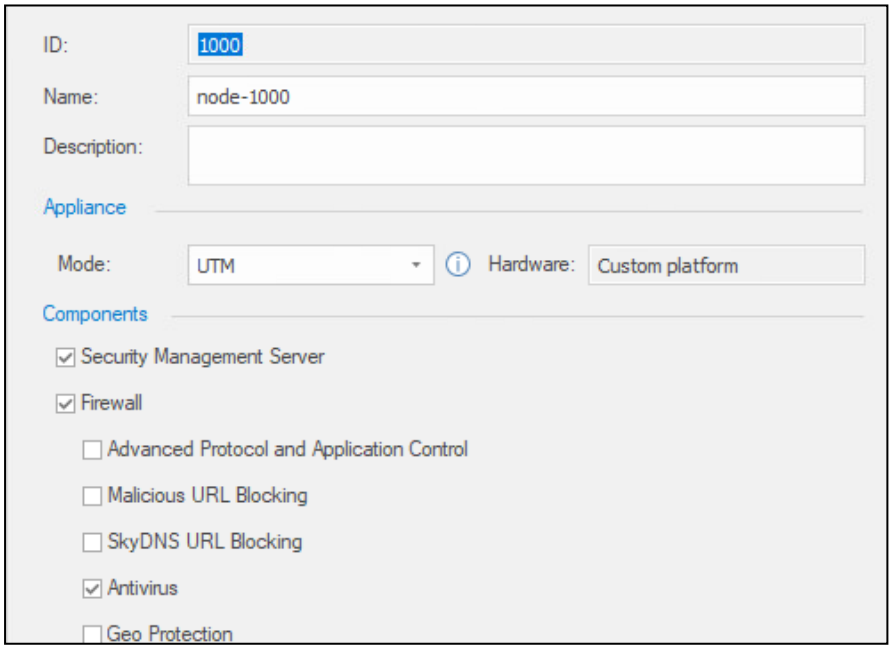
Enable the Antivirus component

Enable the component for those Security Gateways on which the antivirus should operate.

Attention!
An antivirus update license must be linked to the Security Gateway.

To enable the component:

1. In the Configuration Manager, go to **Structure**, select the Security Gateway for which you need to enable the **Antivirus** component and open its properties.
2. In the **Firewall** component, select the **Antivirus** check box and click **OK**.



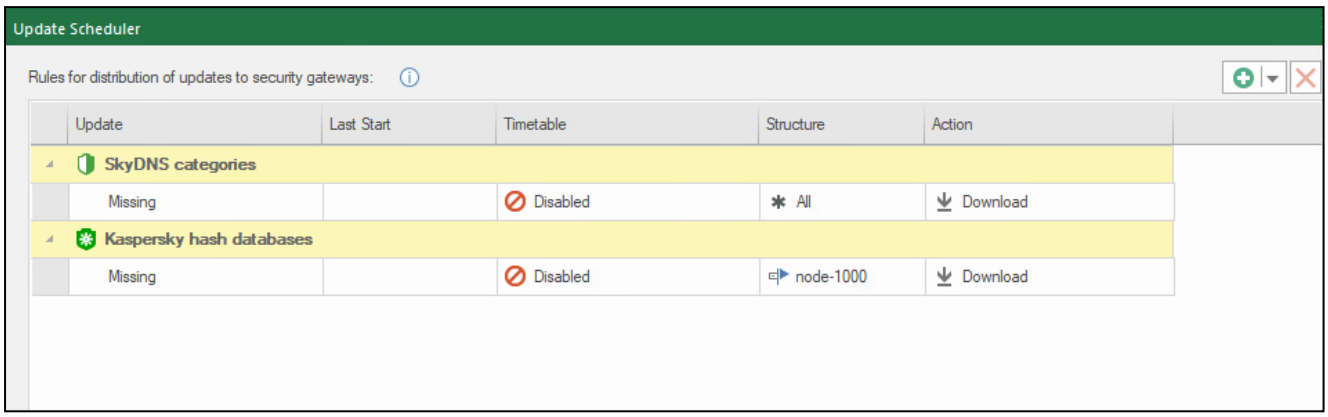
The dialog box closes.

Upload custom hashes to Security Gateways

1. In the Configuration Manager, go to **Administration** and select **Updates**.
2. On the toolbar, click **Update Scheduler**.

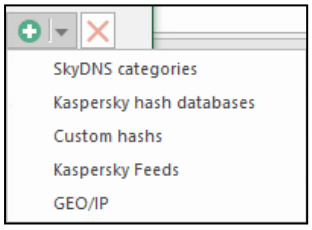
   The respective dialog box appears. It displays Security Gateway update profiles under the following categories:
   - GeoIP country database;

- Kaspersky hash database;
- custom hashes;
- Threat Intelligence feeds;
- SkyDNS categories.

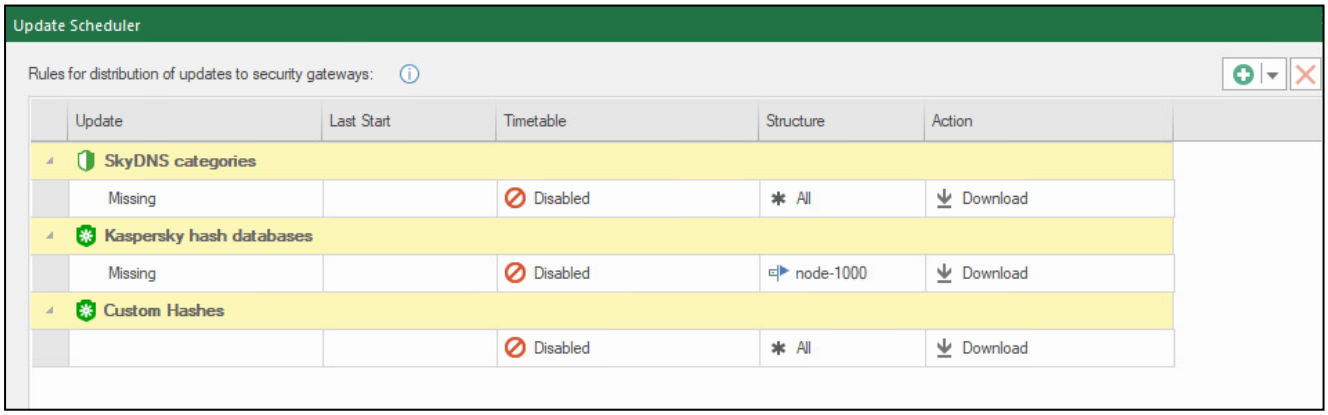


Note.
Since custom hashes were not uploaded to Security Gateways, there is no update profile for custom hashes.

3. To add a custom hash profile, click the arrow to the right of the button.
A list of categories appears.

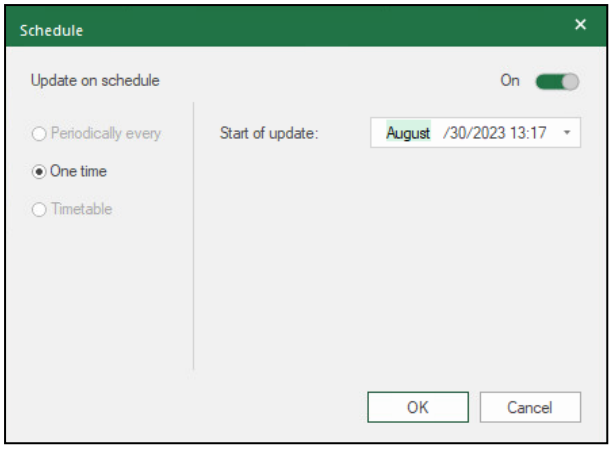


4. Select **Custom hashes**.
The custom hash update profile appears in the profile list.



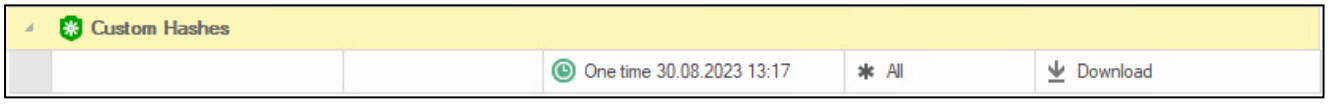
5. Select the custom hash profile and, in the **Timetable** field, click the pop-up button.
The respective dialog box appears.

6. Switch the toggle in the upper-right corner to **On**.
The settings for the update start time become available.



Attention!
For custom hashes, only a one-time update is available, which will be performed in accordance with the time specified in the **Start of update** field.

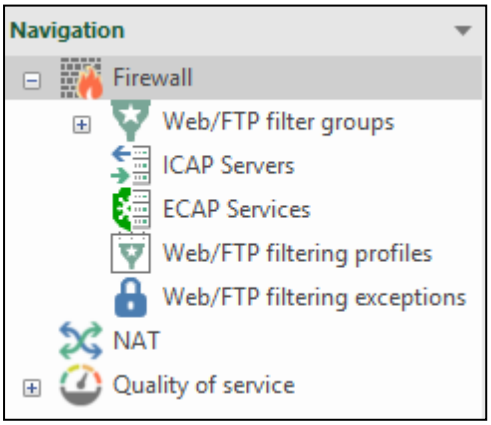
7. Specify the update date and time and click **OK**.
   The dialog box closes and the specified date and time are displayed in the profile.



8. In the **Security Gateways** field, click the pop-up button.
   A dialog box with a list of registered Security Gateways appears.
9. Select the check boxes of those Security Gateways on which you need to install the custom hash update, then click **OK**.
   The Security Gateways are displayed in the profile.

Configure ECAP services

You can configure ECAP services in the Configuration Manager in **Access control** | **Firewall** | **ECAP Services**.



When you go to **ECAP Services**, a list of created ECAP services appears. It contains the following parameters:

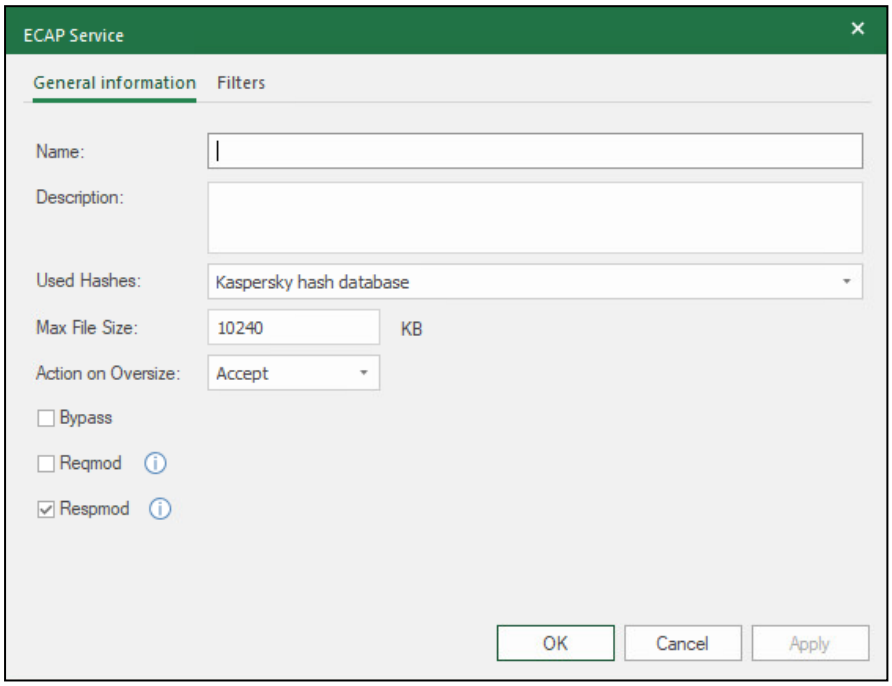
- **Name** — an ECAP service name;
- **Content** — a list of MIME type data sent to an ECAP service;
- **File Extensions** — a list of data types sent to an ECAP service;
- **Description** — an arbitrary service description.

Configuring an ECAP service includes the following procedures:

- create a new service;
- copy a service;
- delete a service;
- view and edit service parameters.

To create a new ECAP service:

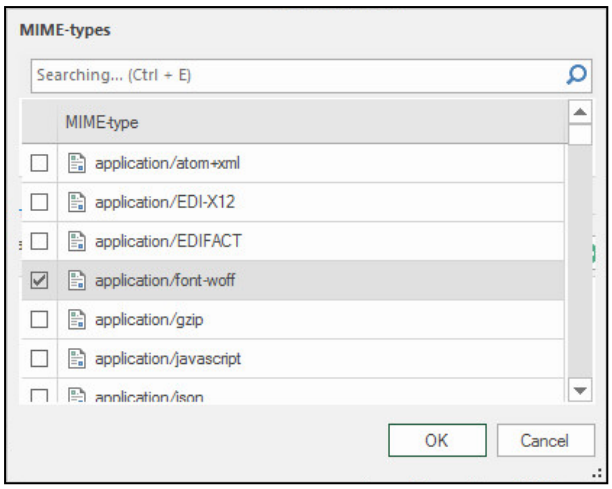
1. On the navigation panel, select **ECAP Services** and click **ECAP service** on the toolbar.
   The **ECAP Service** dialog box appears.



2. On the **General information** tab, specify the required ECAP service parameters.

Parameter	Description
Name	ECAP service name specified by the user
Description	Brief description
Used Hashes	Choice of the database which hashes must be used. The following options are available: • Kaspersky hash database; • custom hashes; • Kaspersky hash database + custom hashes.
Max File Size, KB	Maximum size of a file sent for verification
Action on Oversize	Action that defines what to do if the file size exceeds the limits: • Accept; • Deny
Bypass	If a server is unavailable at the moment, the system bypasses traffic without verification
Reqmod	Request modification mode. This mode is used for scanning outgoing web requests before users send them to file servers such as Gmail and Outlook
Respmode	Response modification mode. The service of response modification analyzes inbound client requests. A response received from the source server content is scanned for malicious content before it is delivered to a user who made a request

3. On the **Filters** tab, create a list of MIME type data if necessary:
   - To add new data types to the list, click  and specify the required **MIME-types** parameters, then click **OK**. You can use the **<Ctrl>**/**<Shift>** + **<Space>** key combination for multiple choice.



- To delete an element from the list, select a MIME type and click ☒.

4. If necessary, specify the respective file extensions by which filtering will be performed. Examples of such extensions:

Description	Example
By one extension	exe
By several extensions	exe,zip,jpg
	exe, zip, jpg
	exe, .zip, .jpg

5. After configuring the **ECAP Service** parameters, click **OK**.
   The **ECAP Service** dialog box closes and the respective record appears in the list.
6. Include the created ECAP service in the WEB/FTP profile.

To copy an ECAP service:

1. On the navigation panel, go to **ECAP Services**.
   In the display area, the list of ECAP services appears.
2. Select the required service and click **Copy** on the toolbar.
   The **ECAP Service** dialog box appears. All parameters will be the same as on the copied service except for the **Name** and **Description** fields.
3. Specify the required parameters.
4. Click **OK**.
   The **ECAP Service** dialog box closes and the respective record appears in the list.

To delete an ECAP service:

1. On the navigation panel, go to **ECAP Services**.
   In the display area, the list of ECAP services appears.
2. Select the required service and click **Delete** on the toolbar.
   A dialog box prompting you to confirm the operation appears.
3. Click **Yes**.
   The service is deleted from the list.

To edit the service parameters:

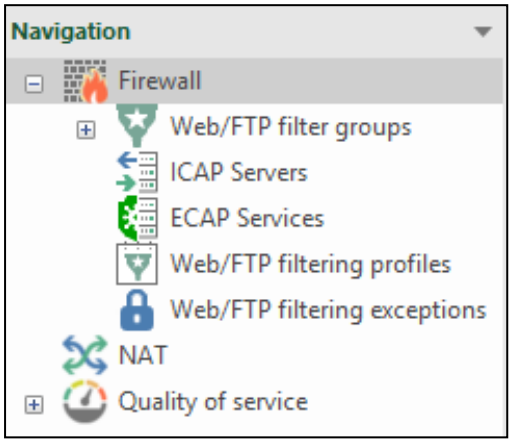
1. Select the required ECAP service and click **Properties** on the toolbar.
   The **ECAP Service** dialog box appears.
2. Edit the required parameters and click **OK**.
3. Save the Security Management Server configuration.

Integration with ICAP

You can add addresses of external ICAP servers to WEB/FTP filtering profiles to check traffic for viruses. In this case, a traffic copy is processed on the ICAP server, which returns the result to the Security Gateway that determine whether to block or pass the traffic further.

To configure ICAP servers:

- In the Configuration Manager, go to **Access control** | **Firewall** | **ICAP Servers**.



When you go to **ICAP Servers**, the list of created ICAP servers appears. It contains the following parameters:

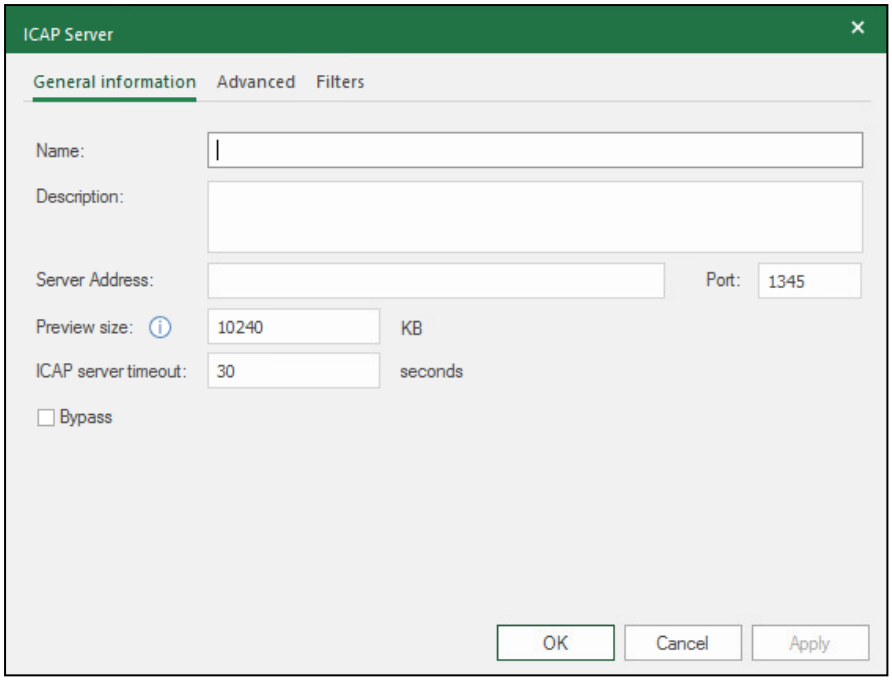
- **Name** — ICAP server name;
- **Address** — server IP address;
- **Port** — port number of ICAP server connection;
- **Content** — list of MIME type data sent to an ICAP server;
- **File Extensions** — list of data types sent to an ICAP server;
- **Description** — arbitrary server description.

Configuring an ICAP server includes the following procedures:

- create a new server;
- copy a server;
- delete a server;
- view and edit server parameters.

To create an ICAP server:

1. On the navigation panel, select **ICAP Servers** and click **ICAP server** on the toolbar.
   The **ICAP Server** dialog box appears.



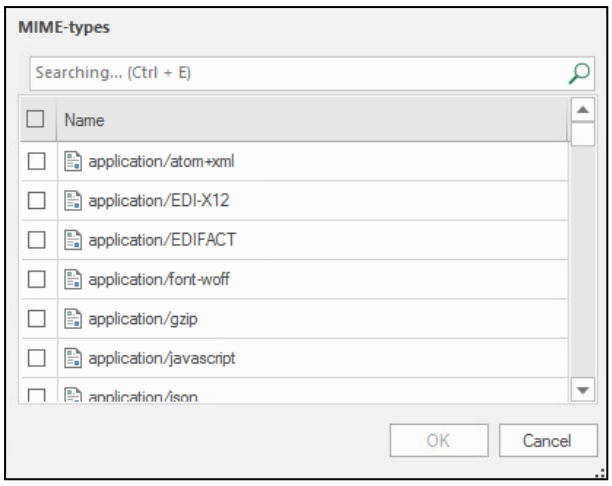
2. On the **General information** tab, specify the required parameters:

Parameter	Description
Name	An ICAP server name specified by a user
Description	Arbitrary description
Server Address	ICAP server IP address
Port	Port number of ICAP server connection
Preview size, KB	The maximum number of the first N bytes of a file that will be transferred on request from the ICAP server
ICAP server timeout, seconds	Timeout after which the Security Gateway stops waiting a response about file security (in case the ICAP server is unavailable)
Bypass	If the server is unavailable at the moment, the system bypasses traffic without verification

3. On the **Advanced** tab, specify additional parameters:

Parameter	Description
Reqmod	Request Modification. Used to process outgoing traffic
Path to Service	Path on the ICAP server to work in **Reqmod -/path** mode
Respmod	Response Modification. Used to process incoming traffic
Path to Service	Path on the ICAP server to work in **Respmod -/path** mode
Send User Name	Enables name sending to the ICAP server
Title	Title that is displayed when sending a user name
Encode to Base64	Name encoding in base64 when using non-standard characters in names
Send IP address	Enables sending the IP address to the ICAP server
Title	Title that is displayed when sending an IP address

4. On the **Filters** tab, create a list of MIME type data if necessary.
   - To add new data types to the list, click  and specify the required **MIME-types** parameters, then click **OK**. You can use the **<Ctrl>**/**<Shift>** + **<Space>** key combination for multiple choice.



- To delete an element from the list, select a MIME type and click ☒.

5. If necessary, specify the respective file extensions by which filtering is performed. Examples of such extensions:

Description	Example
By one extension	exe
By several extensions	exe,zip,jpg
	exe, zip, jpg
	.exe, .zip, .jpg

6. After configuring the ICAP server, click **OK**.
   The **ICAP Server** dialog box closes and the respective record appears in the list.
7. Include the created ICAP server to the WEB/FTP profile.

To copy an ICAP Server:

1. On the navigation panel, go to **ICAP Servers**.
   In the display area, the list of ICAP Servers appears.
2. Select the required server and click **Copy** on the toolbar.
   The **ICAP Server** dialog box opens. All parameters will be the same as in the copied server except for the **Name** and **Description** fields.
3. Specify the required parameters.
4. Click **OK**.
   The **ICAP Server** dialog box closes and the respective record appears in the list of servers.

To delete an ICAP Server:

1. On the navigation panel, go to **ICAP Servers**.
   In the display area, the list of ICAP Servers appears.
2. Select the required server and click **Delete** on the toolbar.
   The dialog box prompting you to confirm the operation appears.
3. Click **Yes**.
   The server will be deleted from the list.

To edit the Service parameters:

1. Select the required ICAP Server and click **Properties** on the toolbar.
   The **ICAP Server** dialog box appears.
2. Edit the required parameters and click **OK**.
3. Save the Security Management Server configuration.

Manage connections

Managing connections includes the following:

- managing related connections tracking through certain protocols (see below).
- viewing and deleting connections created on a Security Gateway in the local menu (see p. **73**).
- configuring connection rematch after installing a policy in the Configuration Manager (see p. **74**).

Related connection tracking

Continent provides a mechanism of tracking related connections. Its functions include the following: when initializing any connection that requires traffic passing through the Security Gateway, Firewall and NAT rules are created on the Security Gateway automatically for related connections.

While Firewall is enabled, the tracking of the related connections is performed for the following protocols:

- FTP;
- GRE/PPTP;
- H.323;
- SIP;
- TFTP.

Tracking related connections excludes the proper work of the protocol inspection mechanisms.

Disabling related connections tracking is provided on the Security Gateway. That ensures the protocol inspection mechanisms.

Disabling can be performed for the Firewall filtering rules and for the NAT rules as well.

Related connections tracking is enabled by default.

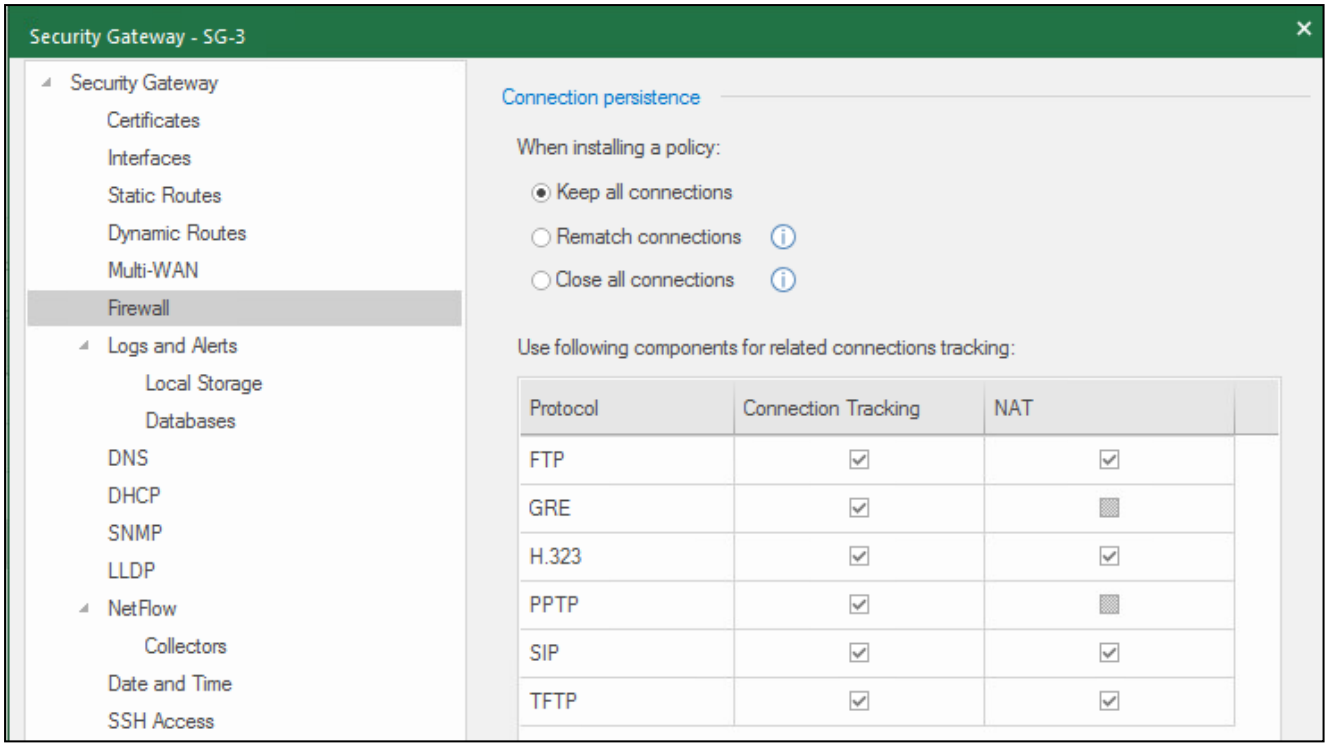
Attention!

While disabling related connections tracking according to some protocol, there must be additional rules for the respective related connections in the list of filtering and NAT rules.

To disable/enable related connections tracking:

1. In the Configuration Manager, go to **Structure**.
2. Select the Security Gateway to disable/enable related connections tracking.
3. On the toolbar, select **Properties**.
4. On the left, select **Firewall**.

   The **Connection persistence** menu appears on the right.



The list of protocols for which disabling related connections tracking is provided.

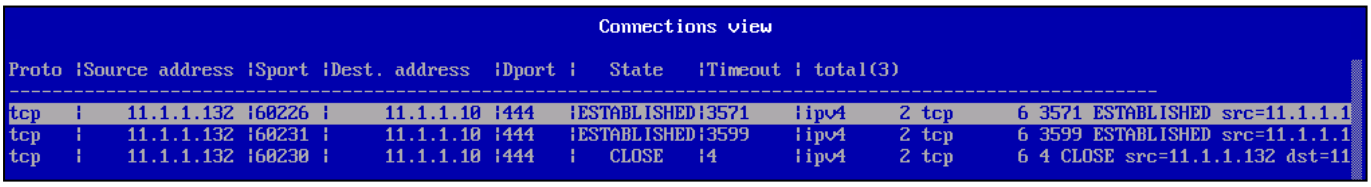
5. To disable/enable related connection tracking of any protocol, delete or select respective parameters in the **Connection Tracking** and **NAT** columns and click **OK**.

View the connection list

To view the list of established connections:

- in the local menu of a Security Gateway, go to **Tools | Diagnostics | Connections view**.

  The list of established connections appears.



Use function keys to execute the following operations:

Key	Operation
F3	Switch between list with the filter applied and the list of all connections
F4	Configure a filter
F5	Update the list of connections
F7	Search by a keyword
F6/F8	Go to the previous/next connection in the list
F12	Clear the list
DEL	Delete a selected connection
ENTER	View details about a selected connection
ESC	Go back to **Diagnostics**

Configure the connection rematch

On a Security Gateway, you can configure connection rematching when installing a policy. In the properties of a service, you can configure whether you want to close connections or keep them when a Firewall rule that uses this service triggers.

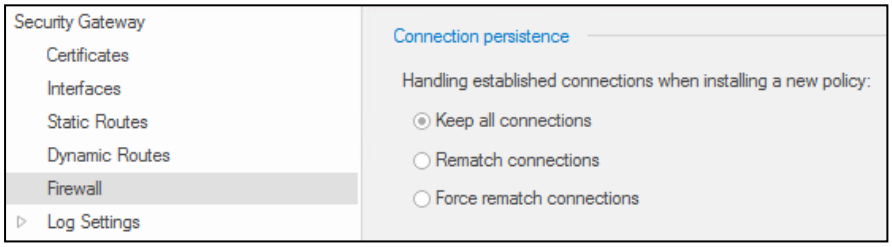
There are three reaction types:

Reaction	Description
Keep all connections	Do not close connections
Rematch connections	Close all connections except those that have the **Keep connections open...** property selected
Force rematch connections	Close all connections including those that have the **Keep connections open...** property selected

To configure connection rematch on a Security Gateway:

1. In the Configuration Manager, select the Security Gateway on which you want to configure connection rematch (the Security Gateway must have the **Firewall** component enabled), click **Properties** on the toolbar and select **Firewall** on the left.

   On the right, connection rematch parameters appear.



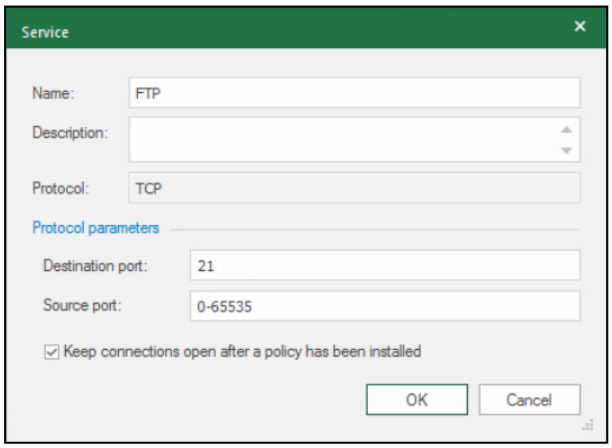
2. Select the required option and click **OK**.

   The dialog box closes.

3. Install the policy on the Security Gateway.

To configure connection rematch in service properties:

1. Open the properties of a required service (see p. **15**).



2. Depending on the requirements, select or clear **Keep connections open after a policy has been installed** and click **OK**.
3. Save the changes.

Attention!

In some cases, changing the connection rematch settings in service properties may have some specifics. The two possible options are described below:

Option 1. Rematch connections is set in the Security Gateway settings, **Keep connections open after a policy has been installed** is set in service properties. After removing the mark in service parameters and applying the policy, the connection rematch for this service does not happen. In this case, change **Rematch connections** to **Force rematch connections** in Security Gateway settings.

Option 2. Rematch connections is set in the Security Gateway settings, **Keep connections open after a policy has been installed** is not set in service properties. After setting the mark in service parameters and applying the policy for this service, the connection closes. If the settings were not changed (**Rematch connections** in Security Gateway settings, **Keep connections open...** in service properties) the next time you apply the policy, the connection rematch for rules including this service does not happen.

Chapter 4
NAT rules

Network address translation (NAT) is the translation of IP packets passing through the Firewall. The translation is performed according to the parameters of a NAT rule. Packets in which IP addresses and ports are translated are defined using the classifiers of NAT rules. The parameters are checked from top to bottom until the first match.

The following NAT types are available:

- **No NAT** — NAT rules are not applied to traffic. It is commonly used as an exception rule to skip network translation on certain traffic.
- **Source** — the source address is translated. In the case of using NAT rules on the Security Gateway (the **Install On** NAT parameter), you can choose an outgoing interface which address will be used for translation.
- **Destination** — the destination address is translated.
- **Hide** (IP Masquerading) — an option of source translation used for providing Internet access. It is the translation of several addresses or one address into the Security Gateway outgoing interface address. The outgoing interface is chosen according to the routing table.
- **One-to-one** — the source address is translated in one-to-one mode. It is available to translate either one network object to another one or one subnet to another one (sizes of the subnets must be the same). Subnets IP addresses are matched in succession: the first address of the source subnet is translated to the first address of the transformed subnet, the second to the second and so on.

The translation is performed for the IP packet that corresponds to all parameters of the NAT rule. The parameters are checked until the first match according to the list of the NAT rules created in the Configuration Manager.

Note.
The NAT rule parameters are joined together using the **AND** logical operator.

To create a NAT rule:

1. Create the respective Security Management Server objects (see p. **12**) that will be used as parameters for the NAT rule:
   - network objects;
   - services;
   - DNS names;
   - countries.

   Note.
   The **DNS names** and **Countries** elements are used as NAT rule parameters only in source packets.
2. Create a NAT rule (see below) and, if necessary, the respective Firewall rule (see p. **33**).

Manage NAT rules

You can manage NAT rules using the shortcut menu commands or the respective buttons on the toolbar.

To open a list of NAT rules:

- In the Configuration Manager, go to **Access control** | **NAT**.

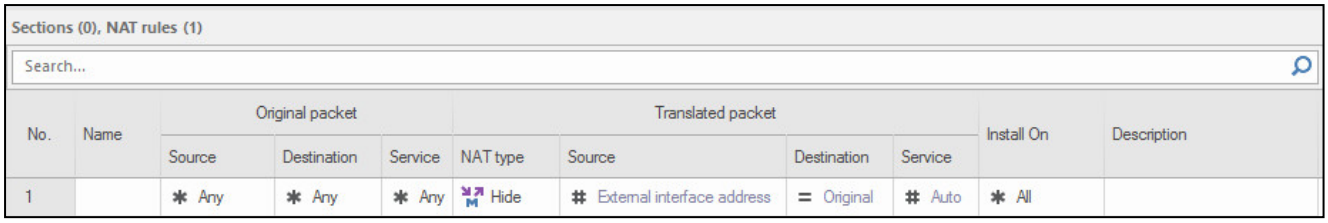
  The list of NAT rules is displayed as a table. Each line of the table represents a single rule. The table columns contain the rule parameters.

Attention!
An IP packet is processed by the first rule that matches the packet.

To create a rule:

- in the list of rules, right-click the **No.** column and click the respective command for creating rules. You can also use the buttons on the toolbar.

  A new rule appears in the table. It has default parameters.



To manage NAT rules:

- NAT rules are managed the same way as the filtering rules (see p. **34**).

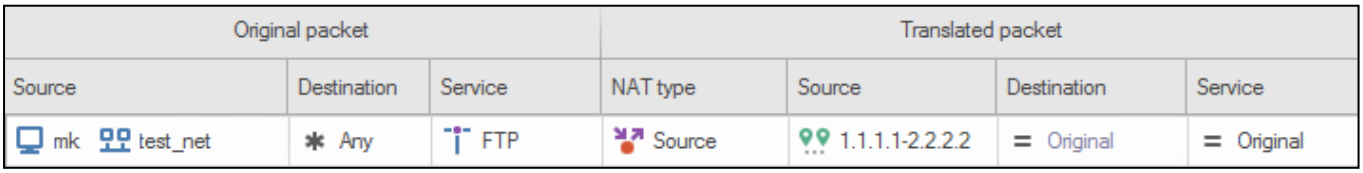
NAT rule parameters

Parameter	Description
№	Sequence number of a rule in the list
Name	Name of a rule
Interface	Can be specified if in the **Install On** parameter a certain Security Gateway was specified. In a sNAT rule — the interface through which a processed packet is sent. In a dNAT rule — the interface through which the processed packet should be received. If there is no interface, this means that parameter is not used in a rule.
Install On	Set of the Security Gateways on which the rule is installed
Description	Additional information (optional)
Original packet	
Source	Displays a name of a network object (group of network objects). Determines the sources of the packets affected by the rule
Destination	Displays a name of a network object (group of network objects). Determines the destinations of the packets affected by the rule
Services	Set of services (group of services). Determines the properties of IP packets affected by the rule
Translation packet	
NAT type	Translation mode
Source	Value depends on the translation mode (see below)
Destination	Destination IP address after translation
Service	Source/destination ports

The **Source** value vary depending on translation mode:

- **No NAT** — no change.
- **Hide** — the outbound interface IP address.
- **Source** — the network object is selected from a group.
- **Destination** — no change.
- **One-to-one** — the network object is selected from a group.

If source translation is required in a large network, use the **address range** object in the **Source** field as a network object in a translated packet.



Examples of using NAT rules

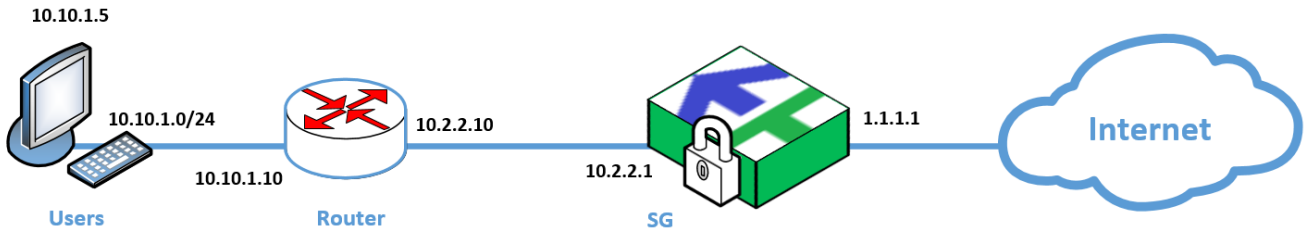
This paragraph contains examples of using NAT rules in the modes described above.

Attention!
For rules with Internet access to work, client hosts must have DNS servers configured and have access to them. The examples below do not display these rules to simplify the examples. Besides, the routes must be configured.

Hide NAT

To provide Internet access, the **Hide** (IP masquerading) mode is used.

As private addresses are not routed to the Internet, it is required to translate private addresses to public ones to provide the private networks with Internet access. To do so, the **Hide** NAT type is used when the chosen addresses are replaced with the external Security Gateway IP addresses.



In the example, access to the Internet of the internal 10.10.10.0/24 network is provided when the private host addresses of this subnetwork are replaced with the Security Gateway outgoing interface address.

For such access to work, a NAT rule and a Firewall rule that allow access to the outside are required. The Firewall rule allowing access from the internal network to the outside has the following parameter values:

Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
10.0.0.0/8	Any	Any	Any	Accept	None	Off	Always	Log	All

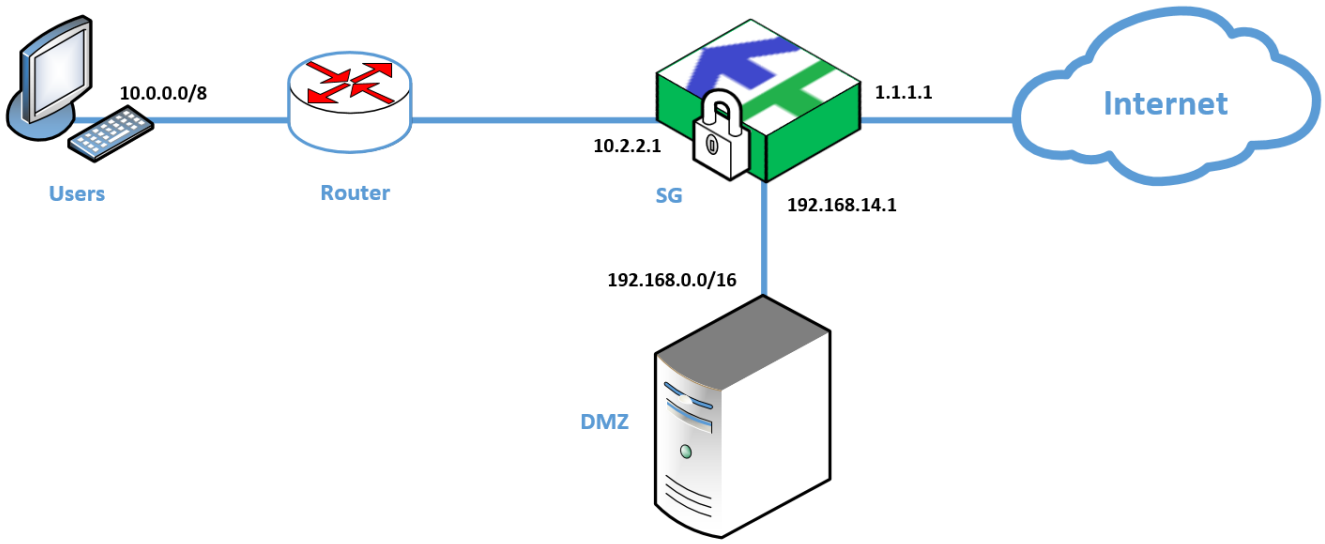
During access from the internal network to the outside, the NAT rule replaces the private IP address with a public IP address (the address of the external interface of the Security Gateway). The NAT rule in this example has the following parameter values:

Original packet			Translated packet				Interface	Install On
Source	Destination	Service	NAT type	Source	Destination	Service		
10.0.0.0/8	Any	Any	Hide	Outbound interface address	Original	Auto	Auto	All

Note that such rules are usually located at the end of a list. We recommend adding private NAT rules (for hosts or small subnetworks) to the top of the list.

No NAT

To exclude addresses from the NAT rules, the **No NAT** mode is used.



In this example, the internal addresses of the protected network are not translated when internal users have access to DMZ. And they are translated if users are connected to the Internet.

The Firewall rules allowing access from the internal network to DMZ and the outside have the following parameter values:

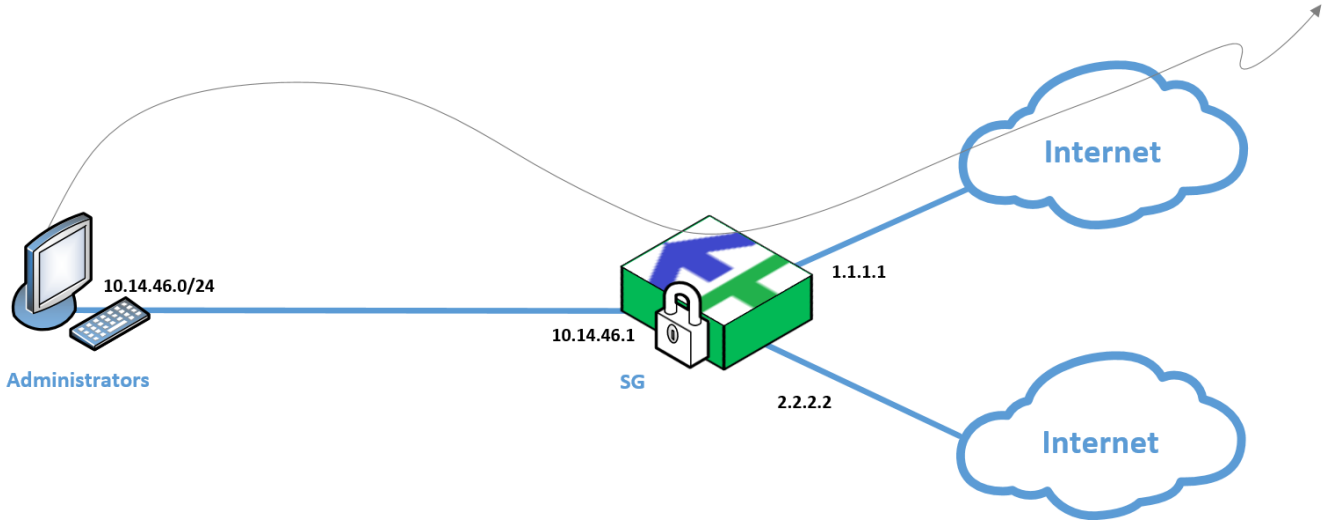
Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
10.0.0.0/8	192.168.0.0/16	Any	Any	Accept	None	Off	Always	Log	All
10.0.0.0/8	Any	Any	Any	Accept	None	Off	Always	Log	All

During access from the internal network to DMZ, NAT rules do not translate IP addresses. During access from the internal network to the outside, the **Hide** NAT type is used. The NAT rules in this example have the following parameter values:

Original packet			Translated packet				Interface	Install On
Source	Destination	Service	NAT type	Source	Destination	Service		
10.0.0.0/8	192.168.0.0/16	Any	No NAT	Original	Original	Original	Auto	All
10.0.0.0/8	Any	Any	Hide	Outbound interface address	Original	Auto	Auto	All

Source NAT with selecting Security Gateway interface

Source NAT with selecting Security Gateway interface is used, for example, in case you need to allow user access to the Internet from a specific external interface. In this example, the administrators gain access to the Internet only via one of the external communication channels.



You need to create a source NAT rule, select the Security Gateway on which this rule will work, then select the interface using which the user will access the Internet in the **Interface** field.

The Firewall rule allowing access from the internal network to the outside has the following parameter values:

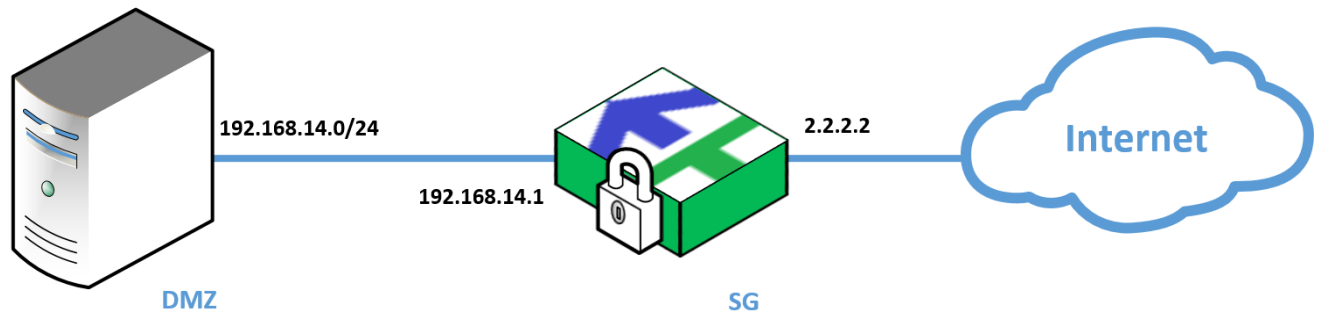
Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
10.0.0.0/8	Any	Any	Any	Accept	None	Off	Always	Log	All

The NAT rule grants access from a specific workstation via the selected external interface. The NAT rule in this example has the following parameter values:

Original packet			Translated packet				Interface	Install On
Source	Destination	Service	NAT type	Source	Destination	Service		
10.14.46.0/24	Any	Any	Source	1.1.1.1	Original	Original	Select external from the list	Security Gateway

Destination translation (resource publication)

You need to make a web-application server public. The tcp/443 port on the Security Gateway is occupied by another service.



When visiting the Security Gateway interface address through the tcp/8443 port, the connection is redirected to the application server in DMZ with substitution of the destination port for tcp/443, i. e. the destination NAT is performed.

The Firewall rule allowing access from the outside to the external address of the Security Gateway on which the application server will be published has the following parameter values:

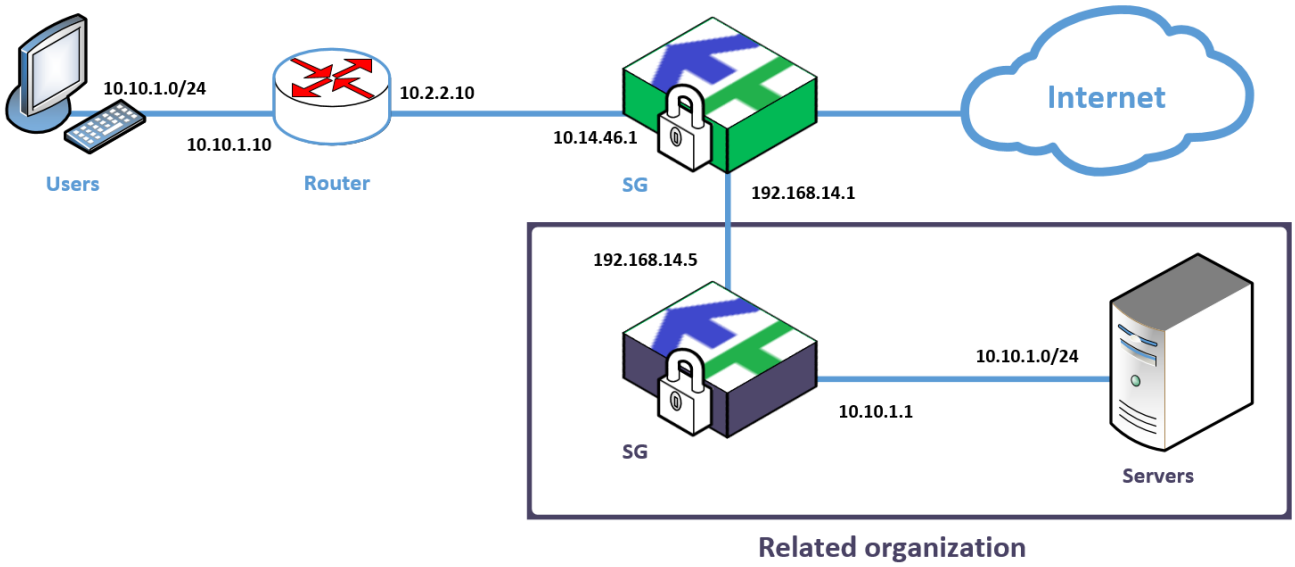
Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
Any	2.2.2.2	tcp_8443	Any	Accept	None	Off	Always	Log	All

The NAT rule redirects the external traffic to the server in DMZ by changing the destination port. The NAT rule in this example has the following parameter values:

Original packet			Translated packet				Interface	Install On
Source	Destination	Service	NAT type	Source	Destination	Service		
Any	2.2.2.2	tcp_8443	Destination	Original	192.168.14.25	tcp_443	Auto	All

Source, destination and destination port translation

This example provides simultaneous source and destination address translation. This may come in handy if you need to get access to the server in a related organization, but addressing there is the same and the destination port (**tcp/443**) is occupied on the Security Gateway in the protected network. The related organization has set a condition to accept traffic for this purpose on port **tcp/9443**, but it is also occupied on our Security Gateway, so our users will access **tcp/10443** and the Security Gateway will translate these addresses.



A user from the **10.10.1.0/24** protected network wants to get access to the server in the related organization, which in turn is also located in the **10.10.1.0/24** subnet. To ensure user access, you can use double NAT. To do so, create two NAT rules:

- NAT rule 1 — destination and destination port translation.
- NAT rule 2 — source translation.

This order is determined by the traffic processing scheme, since the destination translation is processed before the source translation.

The user will access the IP address of our Security Gateway (**10.14.46.1**) via **tcp/10443** port, and the destination address will be replaced by the IP address of the Security Gateway of the related organization (**192.168.14.5**), the port will be replaced by **tcp/9443**, then the source will be replaced by the address of our Security Gateway in the related network (**192.168.14.1**).

The Security Gateway of the related organization will accept the connection to its address via the **tcp/9443** port and retranslate the traffic to the required server via the required port.

In the Security Gateway within the protected network, the NAT rule 1 translates the destination address and the destination port, the NAT rule 2 translates the source address. In the NAT rule 2, you need to specify the already translated address as destination, and the already translated port as service.

The Firewall rules are created for the original traffic and have the following parameter values:

Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
10.10.1.0/24	10.14.46.1	tcp_10443	Any	Accept	None	Off	Always	Log	All

The NAT rule 1 is created for the original traffic, the NAT rule 2 is created for the traffic translated by the NAT 1 rule. In this example, the destination in the **10.10.1.0/24** network is replaced by **192.168.14.5**, hence the NAT rule 2 has **192.168.14.5** as the destination. The NAT rules in this example have the following parameter values:

Original packet			Translated packet				Interface	Install On
Source	Destination	Service	NAT type	Source	Destination	Service		
10.10.1.0/24	10.14.46.1	tcp_10443	Destination	Original	192.168.14.5	tcp_9443	Auto	All
10.10.1.0/24	192.168.14.5	tcp_9443	Source	192.168.14.1	Original	Original	Auto	All

On the Security Gateway of the related organization, you need to create the Firewall rule with the following parameter values:

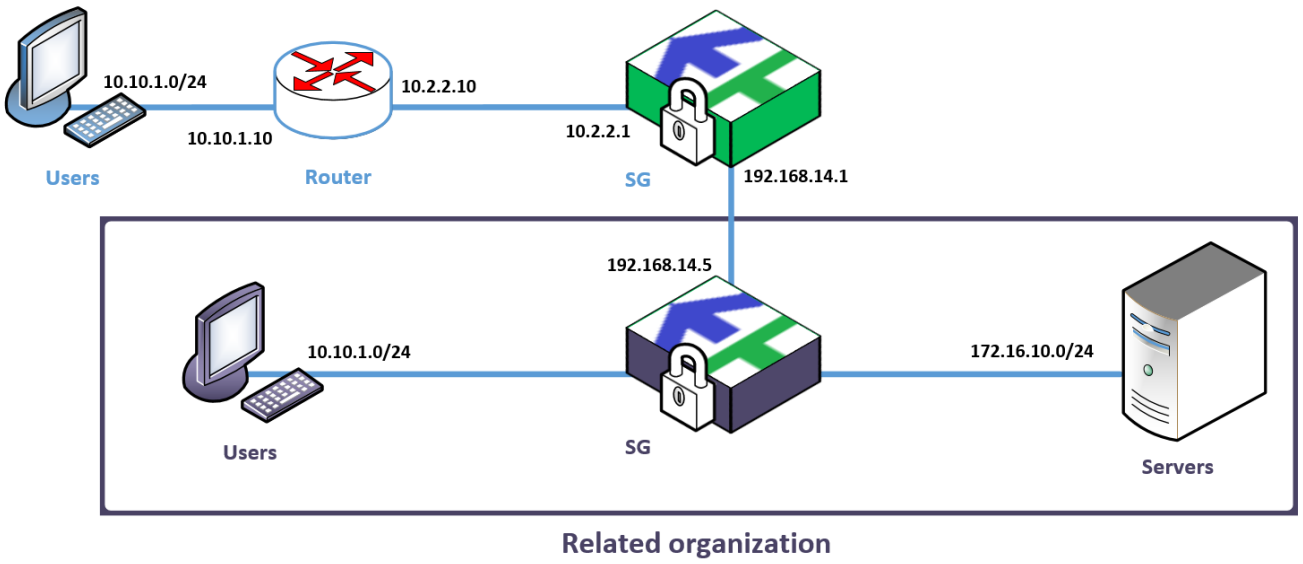
Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
192.168.14.0/24	192.168.14.5	tcp_9443	Any	Accept	None	Off	Always	Log	All

The destination NAT rule replaces the **9443** port with **443** and destination with the server address (**10.10.1.30**). The NAT rule in this example has the following parameter values:

Original packet			Translated packet				Interface	Install On
Source	Destination	Service	NAT type	Source	Destination	Service		
192.168.14.5	192.168.14.5	tcp_9443	Destination	Original	10.10.1.30	tcp_443	Auto	All

One-to-one NAT

The **One-to-one** mode is used in overlapping networks. For example, if the same subnetworks are used both in our and a related organization, and what is more, it is unavailable to change the addressing. In this case, all the addresses from the specific pool can be matched in succession to other addresses when getting access to the network of the related organization.



In this example, the 10.10.1.0/24 subnetwork is used both in our organization and in the related one. To provide our users with the access to the Partner network, it is required to translate addresses to the pool selected by the related organization. In case of the **One-to-one** translation, all ports are translated.

On the Security Gateway of our organization, you need to translate the **10.10.1.0/24** subnet to **192.168.111.0/24**.

The Firewall rule has the following parameter values:

Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
10.10.1.0/24	172.16.10.0/24	Any	Any	Accept	None	Off	Always	Log	All

The NAT rule has the following parameter values in this example:

Original packet			Translated packet				Interface	Install On
Source	Destination	Service	NAT type	Source	Destination	Service		
10.10.1.0/24	172.16.10.0/24	Any	One-to-one	192.168.111.0/24	Original	Original	Auto	All

On the Security Gateway of the related organization, you need to create a Firewall rule with the following parameter values:

Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
192.168.111.0/24	172.16.10.0/24	Any	Any	Accept	None	Off	Always	Log	All

You do not need to create a NAT rule on the Security Gateway of the related organziation.

Appendix

Install a policy

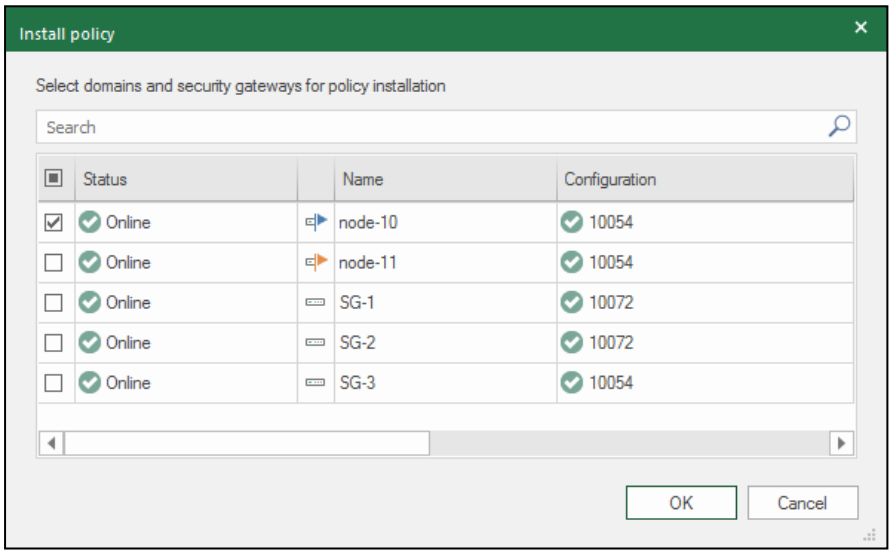
To apply changes in the Security Gateway configuration, install a policy on this Security Gateway. To install the policy, a task is created. Tasks are performed in rotation. The more changes to be applied, the more time is required to perform the task.

To install a policy:

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

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

   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 were added. When the task is performed, the respective icon appears. Then, the task is removed from the **Notification center**.

Keyword search

Continent provides a search of rules by keywords **All** and **Any** and logical operators. The search is performed in each attribute field.

The keyword search is available for the following policies:

- firewall rules;
- NAT rules;
- proxy server rules;

  Note.
  For proxy server policies, it is possible to search only for the keyword **Any** as the policy is set on specific management servers.

- traffic prioritization;
- remote access policies;
- IPS policies.

  Note.
  For IPS policies, it is possible to search only for the keyword **All**.

The search allows the use of the **AND**, **OR** (or the space character between object names) and **NOT** (or the **!** character) logical operators. When using the **!** operator, separate it from the object with a space character, for example: ! Any или ! Hide.

To perform a keyword search:

- Enter a query in the search box of the required Configuration Manager section and press **<Enter>**.

Protocols and ports

This section provides information about ports and protocols used for establishing a connection between Security Gateways.

Security Management Server

Protocol/port	Purpose
TCP/22	SSH connection to the Security Management Server
TCP/80	CRL transfer
TCP/443	Transfer monitoring and audit data between the administrator's workstation and the Security Management Server
	Download update files from the update server to the Security Management Server
	Transfer updates to the Security Gateway
	Monitoring
TCP/444	Connection between the Configuration Manager and the Security Management Server
TCP/4431	Monitoring web interface with GOST encryption
TCP/6666	Control channel between the Security Management Server and the Security Gateway
TCP/8888	Transfer logs from the Security Gateway to the Security Management Server
UDP/67	DHCP on the Security Management Server
UDP/123	NTP data transfer
UDP/161	SNMP data transfer between the administrator's workstation and the Security Management Server
TCP/10000—10255	Data transfer using VPN channels
UDP/3780/4334/5405	Security cluster synchronization data transfer

Security Gateway

Protocol/port	Purpose
TCP/22	SSH connection to the Security Gateway
TCP/80	Authentication Portal
TCP/443	Access Server, Authentication Portal
	Download updates from the Security Management Server
UDP/67	DHCP on the Security Gateway
UDP/123	NTP data transfer
UDP/161	SNMP data transfer between the administrator's workstation and the Security Gateway
TCP/10000—10255	Data transfer using VPN channels
UDP/3780/4334/5405	Security cluster synchronization data transfer

Import network objects from a file

To import network objects, an administrator has to create a file with the **.csv** extension and specify the list of network objects according to a certain data structure. The administrator downloads this file to Continent using the Configuration Manager. The system parser analyzes the list line by line (every line is assigned to a single object), checks data validation and imports the specified network objects to the Security Management Server database.

Attention!
We recommend creating a backup copy of the Security Management Server before importing network objects from external systems.

Structure of the file

First attribute

Specify one of the following objects (value format):

- host IP address (x.x.x.x);
- network IP address (x.x.x.0/x);
- address range (x.x.x.x - x.x.x.x);
- group elements (the number of values depends on the number of elements in the group) (X | X | X ...).

IP addresses must be specified in IPv4 format.

Imported groups must come after other network objects in the list. All elements specified in a group must be in the list or the database. Otherwise, they will not be included in the group.

Second attribute

Specify an object name using valid characters:

- a-z;
- A-Z;
- 0-9;
- `!@#$^()-=_+[]',.

For groups of network objects the name value is required, for other objects — optional (if this object is not included in a group).

Third attribute

Specify the parameter of interaction between groups when the group name is duplicated (only for groups).

If the attribute is empty, the imported group is created with a name with /1 added in the end. If the attribute has ***** value, the groups are combined and the elements from the imported group are added to the group with a duplicate name in the database. If the value is other than *****, Continent treats it as an empty attribute.

Fourth attribute

Specify an object description using valid characters:

- a-z;
- A-Z;
- 0-9;
- `!@#$^()-=_+[]',.

This attribute is optional. If the combine parameter ***** is specified for a group, then the description of the group from the database is saved during import.

Structure of a .csv file

Parameter	First attribute		Second attribute	Third attribute	Fourth attribute
Field in the Configuration Manager	Address	Elements (of a group)	Name	Combine groups parameter (of groups)	Description
Valid values	According to the value format	a–z A–Z 0–9 `!@#$^()-=_+[]',»	a–z A–Z 0–9 `!@#$^()-=_+[]',»		a–z A–Z 0–9 `!@#$^()-=_+[]',»

Example of an import file

IP/ELEMENT	_NAME_	_MIGRATION_	_COMMENT_

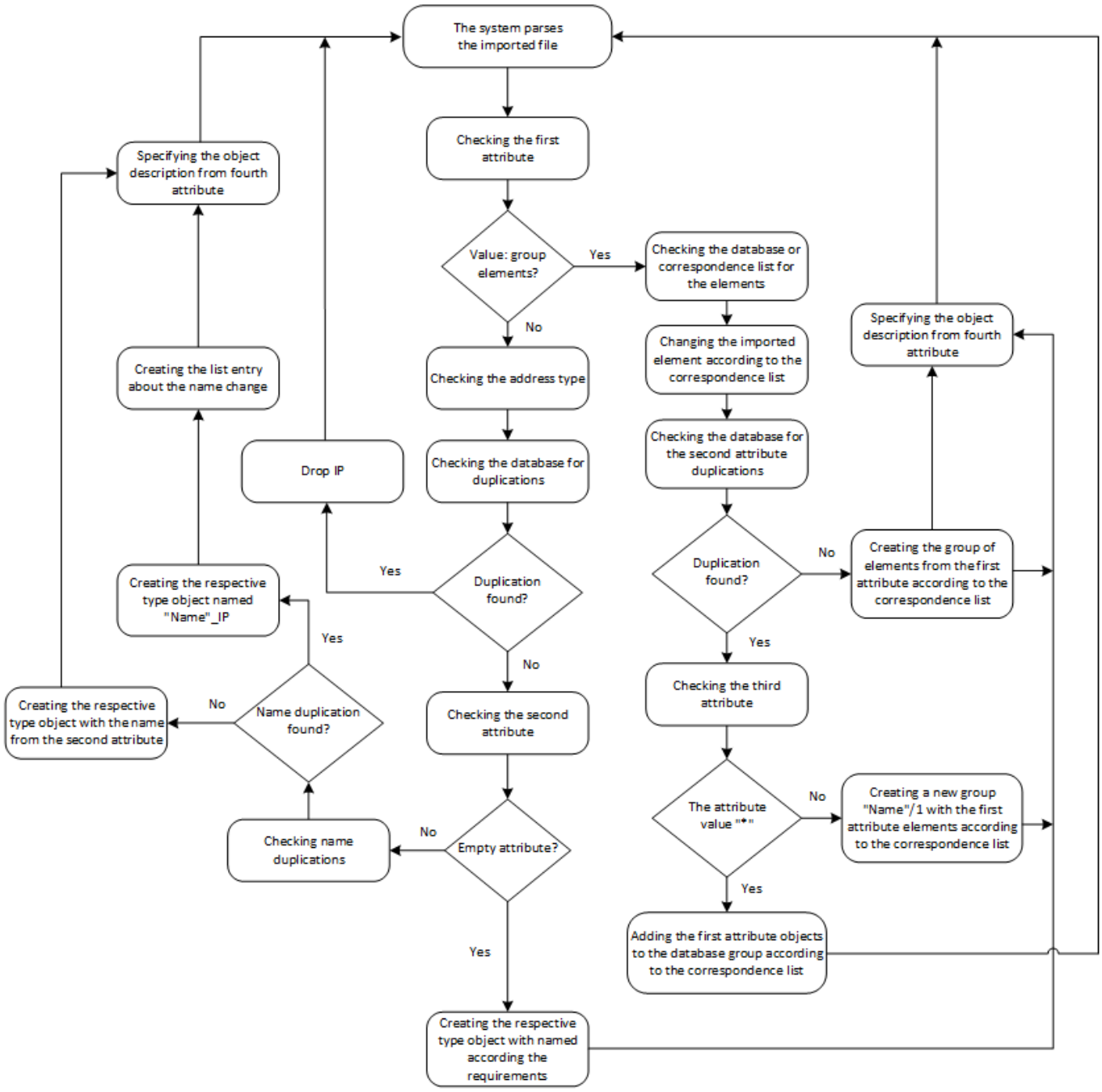
192.168.1.1	User1		Administrator
192.168.1.2	User2		
192.168.1.3	User3		Administrator2
192.168.1.10			
192.168.1.0/24	Network1		Company network1
192.168.2.0/24	Network2		Company network2
192.168.1.101-192.168.1.120	Range1		Users
192.169.1.121-192.168.1.140	Range2		Servers
192.168.1.141-192.168.1.200	Range3		Free pool
User1 | User2 | User3	Group1	*	Admins
Range1 | Range2 | Range3	Group2		PC

Attention!

- The number of processed lines should not exceed **5000** within one process.
- The file cannot include groups containing other groups.
- The groups included in the file cannot be empty (not include any elements).

Import algorithm

1. Continent checks the file coding. If the format is not a text one, an error appears. If the coding is correct, the file is passed to the parser.
2. The parser analyzes the downloaded file line by line. Initially, the parser checks the first attribute and determines the type of an object.
3. If the type of an object is a host, a network or an address range (according to the value format), Continent checks whether a duplicated object exists in the database.
4. If a duplication exists, the parser ignores the value and moves on to the next line. Otherwise, the parser checks the second attribute (object name) in this line.
5. If the attribute is empty (an administrator has not specified the object name), Continent creates an object according to the value format from the first attribute and assigns it a name according to the requirements. The description is also filled with the value from the fourth attribute. Otherwise, a search for duplicate records in the database takes place.
6. If there are no duplicate records, Continent creates an object with the name specified in the second attribute. Otherwise, the name template is **Name_<First attribute value>**. The match list (used if a group includes this object later) also records this change. In both cases, the description is filled with the value from the fourth attribute after creating the object.
7. If the value is a list of group elements at step **2**, each of these elements is searched in the match list and in the database list. Elements which were not found are discarded.
8. Next, Continent checks the second attribute (object name) for duplicate records in the database and, if there are no such records, creates a group with a specified name which includes elements specified in the first attribute (according to the match list). The description is also filled with the value from the fourth attribute.
9. If there are objects with a duplicate name, Continent checks the third attribute, the value of which can be empty. Then Continent creates a new group with the **Name/1** name and includes elements from the first attribute (according to the match list) in it. If the value is *****, elements from the first attribute (according to the match list) are added to the existing group. The description is filled only when there is no combined groups parameter.



Import objects

Before the start of the import, create a **.csv** file according to the description above.

1. In the Configuration Manager, open the list of network objects (see p. **12**).
2. Right-click the blank space in the list of network objects.

   The shortcut menu appears.
3. Select **Import**.

   The File Explorer appears.
4. Specify the path to the created file and click **OK**.

   The import starts and the import progress bar appears.

   Progress is displayed as a percentage of processed objects to the total number of objects. After the operation is completed successfully, you receive the respective message.
5. Click **OK**.

   Import is complete. The new imported objects appear in the list of network objects.

6. Save the changes to the Security Management Server configuration.

Import Firewall rules from the Check Point configuration

In Continent, you can import Firewall rules, NAT rules and related objects from the Check Point configuration versions R77.30 and R80.20. For rule importing tools, see the website https://github.com/itseccode/c4_tools (in Russian).

AH protocol data exchange

To exchange data using AH (IP protocol 51), allow it in the Firewall rule.

To configure a Firewall rule:

1. In the Configuration Manager, go to **Access Control** | **Firewall**.

   The list of Firewall rules appears in the display area.
2. Select a Firewall rule or create a new one by specifying the required parameters (see p. **34**). Click **Add** in the **Service** shortcut menu.
3. Click **Create**.

   The **Service** dialog box appears.
4. Specify **51** in the **Protocol** cell. Specify the **Name** and click **OK**.
5. Select **Skip** in the **Action** shortcut menu.
6. Save changes to the Security Management Server configuration and apply the policy on the required Continent components (see p. **84**).

If AH packets do not pass after installing a policy with the Firewall rule, you need to break existing connections on the required Security Gateways.

To close existing connections:

- in the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Reset sessions** on the toolbar.

Quick replacement of a network object in multiple Firewall and NAT rules

This procedure makes it possible to quickly replace a network object used in all Firewall rules and/or in NAT rules with another one.

To replace a network object:

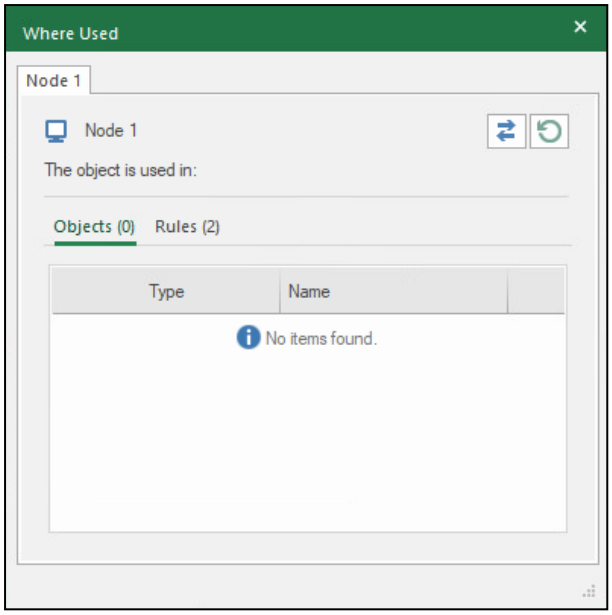
1. Open the list of Security Management Server objects (see p. **12**) or the list of Firewall/NAT rules (see p. **76**).
2. If the list of Security Management Server objects is chosen, select the network object you want to replace.

   If a Firewall/NAT rule is chosen, select the parameter in which the **network object** value is used that you want to replace.

   Right-click it.

   A menu appears.
3. Select **Where Used...**

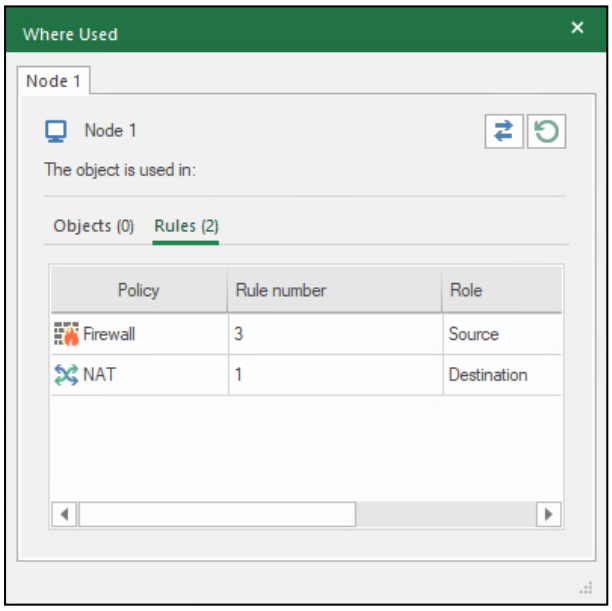
   The **Where Used** dialog box appears.



It contains two tabs: **Objects** and **Rules**.

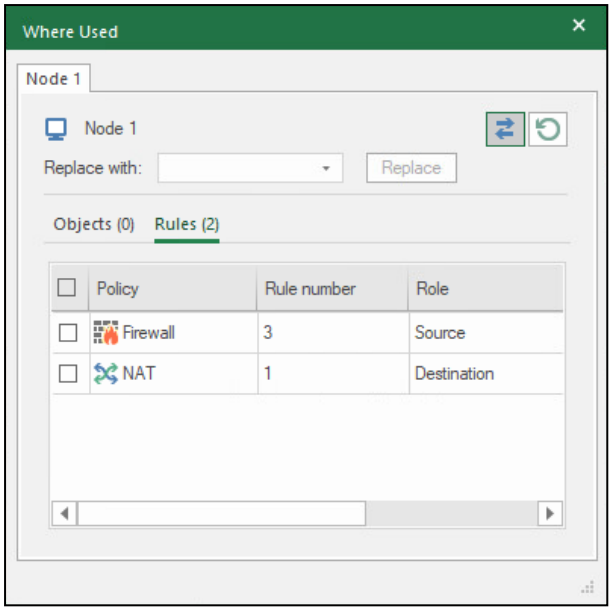
4. Select the **Rules** tab.

   Now you can see policies in which the network object is used: the Firewall (Firewall rules) or NAT rules and their numbers in their lists (in the Firewall rule list and in the NAT rule list).



5. Click  .

   A dialog box appears.

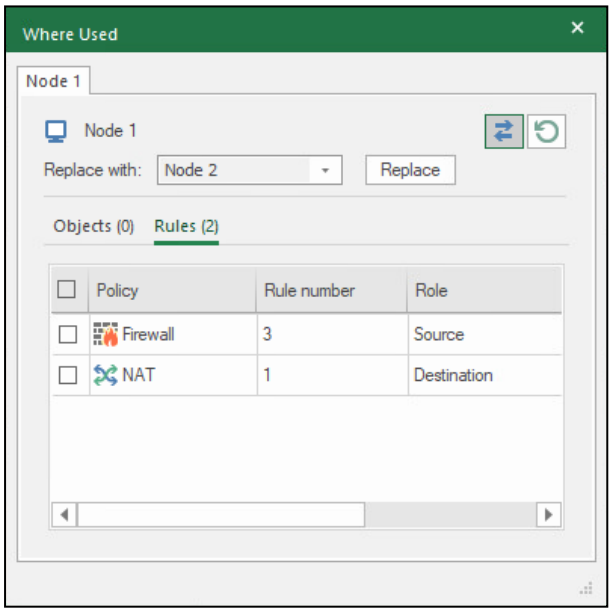


6. In the **Replace with** field, expand the list.

   The list of registered network objects appears.

7. Select the required network object.

   Select the policy in which you want to replace the network object: in the Firewall or in NAT rules. Select the respective check box.



8. Click **Replace**.

   A confirmation message box appears.

9. Click **Yes**.

   The network object will be replaced in all rules of the selected policy.

10. Save the changes.

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Deployment.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Management.
3. Continent Enterprise Firewall. Version 4. Administrator guide. Monitoring and Audit.
4. Continent Enterprise Firewall. Version 4. Administrator guide. VPN.
5. Continent Enterprise Firewall. Version 4. Administrator guide. Networking functions.
6. Continent Enterprise Firewall. Version 4. Administrator guide. Installation and Update.