SECURITY code

Continent Enterprise Firewall
Version 4

Networking Functions

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

ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol
DNAT	Destination Network Address Translation
DNS	Domain Name System
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MD5	Message Digest 5
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
QoS	Quality of Service
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLVS	Type, Length, Value attributes
TTL	Time to live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

Introduction

This manual is designed for administrators of Continent Enterprise Firewall, Version 4 (hereinafter — Continent). It contains information about configuration of networking functions.

This document contains links to documents [**1**] – [**8**].

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.

Network parameters of the Security Gateway

You can configure network parameters of a Security Gateway in the **Properties** window using the Configuration Manager. Depending on the selected section, you can view a respective set of parameters. In the local menu, there is a limited list of these parameters.

Section	Parameters	Note
Security Gateway	Select an operation mode and active components	
Interfaces	Configure physical and virtual interfaces	See p. **7**
Virtual Routing and Forwarding	Configure VRF zones	See p. **42**
Static Routes	Configure static routing tables and metrics	See p. **32**
Dynamic Routes	Configure dynamic routing	See p. **35**
Multi-WAN	Select Multi-WAN mode, manage WAN channels, configure traffic balancing between external interfaces	See p. **23**
QoS	Configure the QoS	See p. **65**
ARP	Configure the ARP	See p. **58**
DNS	Configure IP addresses of DNS servers	See p. **57**
DHCP	Configure a DHCP server role	See p. **72**
SNMP	Configure Security Gateways' monitoring via SNMP	See [**8**]
SSH	Configure remote access to the Security Gateway local menu	See p. **82**
LLDP	Collect data on neighboring devices via LLDP	See p. **87**
NetFlow	Configure the mechanism for exporting data on network traffic passing through the Security Gateway at the flow level	See p. **83**
Date and Time	Configure the time synchronization between Security Gateways using NTP	See p. **78**
Monitoring (only on the Security Management Server)	Configure a connection to an external database for storing monitoring data	See [**6**]
Management Access (only to the Security Management Server)	Configure the list of addresses allowed to connect to the Security Management Server	See [**5**]
ICMP Messaging	Configure the ICMP messaging	See p. **86**

Network interfaces of the Security Gateway

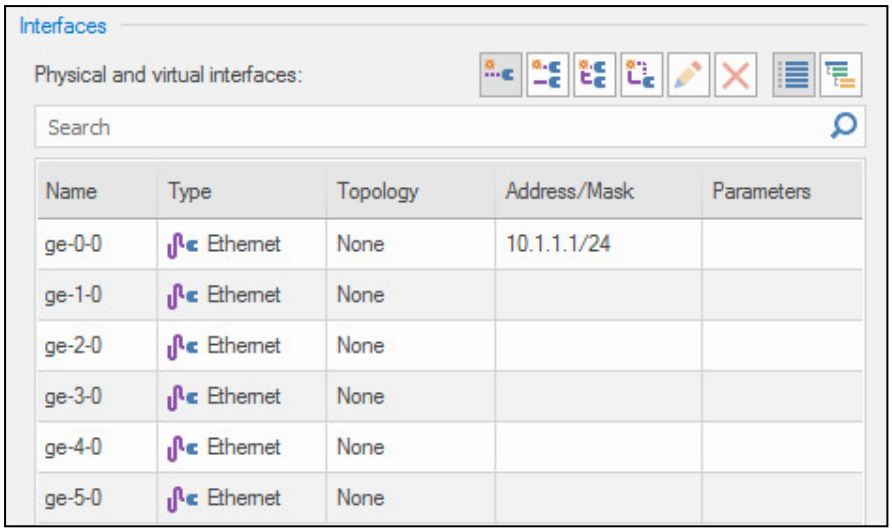
You can configure network interfaces of the Security Gateway using the local menu or the Configuration Manager after you initialize the Security Gateway and connect it to a Security Management Server (see [**2**], **Deployment of Security Gateway**).

You can specify the network interface topology and aggregation only using the Configuration Manager.

To configure network interfaces of a Security Gateway using the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.
2. On the left, select **Interfaces**.

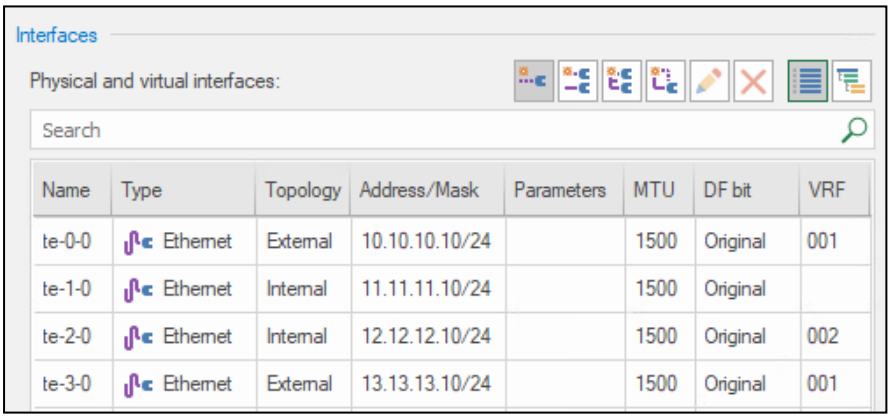
The respective parameters appear on the right.



Any interface can have several IP addresses.

Note.
When working with lists in the Configuration Manager, you can search for a list element you want. The search can be performed by attributes of an element (Security Management Server object, interface, QoS rule, etc.). For this purpose, enter an attribute value or its part in the **Search** field and press <**Enter**>. You can also enter logical expressions using **and**, **or**, **not**, **()**.

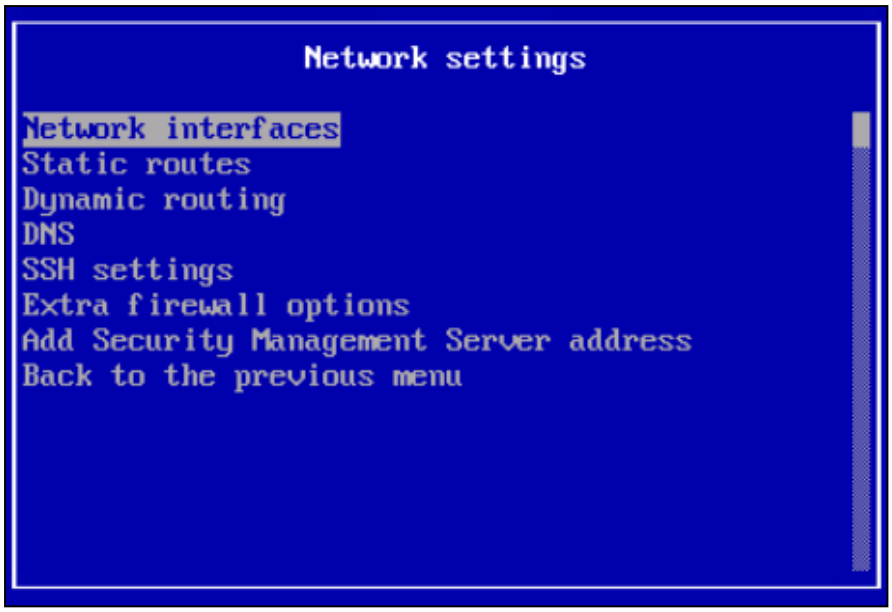
If the Security Gateway is operating in virtual routing mode (VRF zones are configured on the Security Gateway), the list of interfaces includes their VRF zone membership (for more information on VRF zones, see p. **42**).



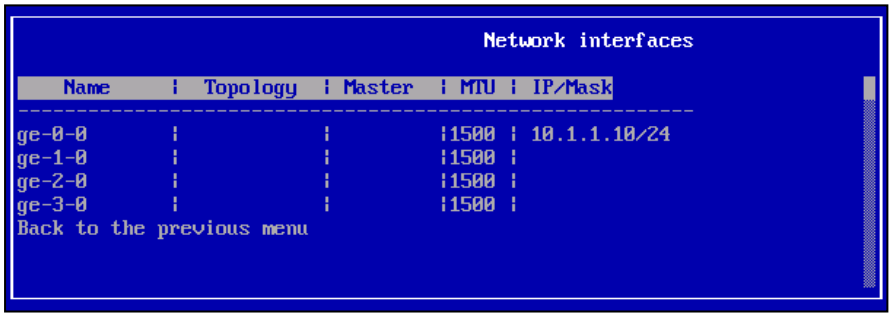
To configure network interfaces using the local menu:

1. In the main menu, select **Settings** and press <**Enter**>.
   The respective menu appears.
2. Select **Network** and press <**Enter**>.

The respective menu appears.



3. Select **Network interfaces** and press <**Enter**>.
   The list of network interfaces appears.



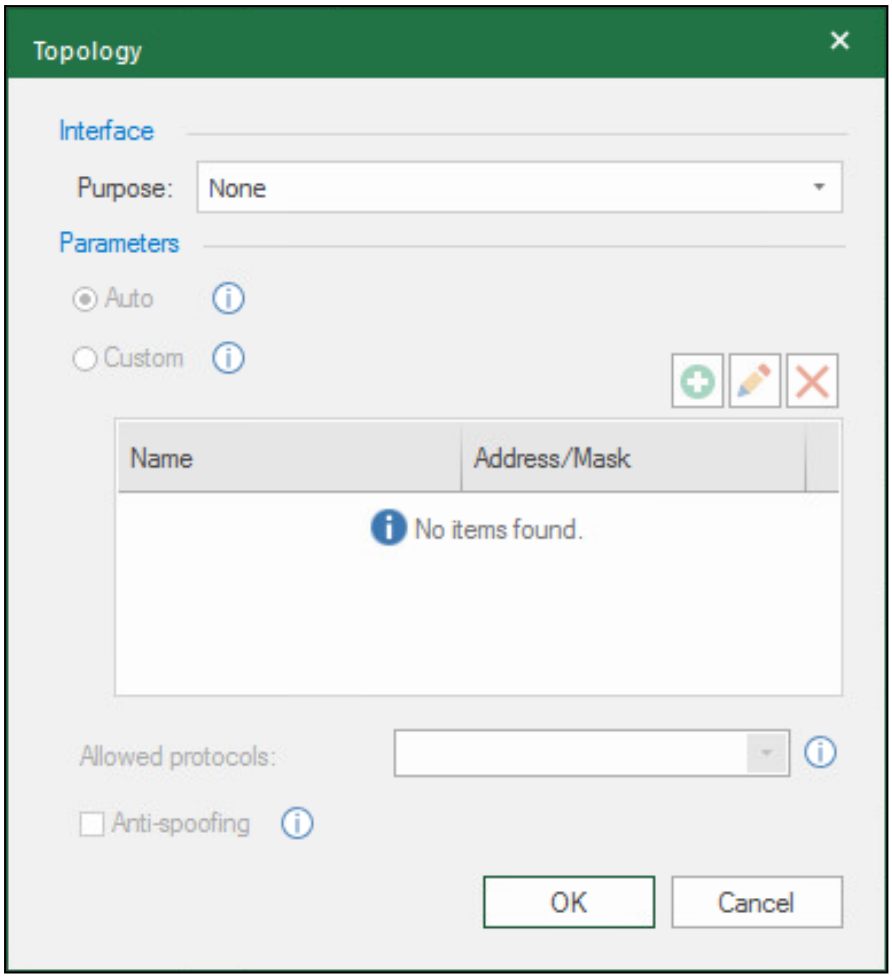
4. After all the parameters are configured, apply local changes on the Security Gateway.
5. Confirm Security Gateway configuration changes in the Configuration Manager (see [**5**]).

Configure network interface topology

To specify the topology for a network interface in the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties**.
   The respective dialog box appears.
2. On the right, select **Interfaces**.
   The list of interfaces appears.
3. Double-click the **Topology** cell related to the required interface line.

The respective dialog box appears.



4. Specify the purpose of the interface according to the table below:

Purpose	Description
Not defined	Set by default unless other types are assigned
Internal	Set, depending on the component in which this interface is used, for example, in DHCP settings or in L3VPN settings (for connection to a protected network)
External	Set, depending on the component in which this interface is used, for example, in L3VPN settings. Communications with the Internet. You can set more than one external interface
Monitoring	Traffic analysis in Monitor mode (only for High Perfomance FW mode)
Inline	Traffic analysis in Inline mode (only for High Perfomance FW mode)
Switch port	Communications with a protected network through L2VPN

5. For internal and external interfaces, you can select **Anti-spoofing** to protect IP address from spoofing if necessary.

   The **Parameters** settings become available for editing.

6. If you have selected **External**, select the routing type (**Auto/Custom**).
   - If you select **Auto**, the topology for an external interface is built automatically according to RFC1918.
   - If you select **Custom**, the topology is built automatically based on a network objects user list and the IP addresses of a private network (RFC1918). The network objects user list contains private network IP address exclusions

   Note.
   In this case, the system filters physical interfaces according to RFC1918 using the **10.0.0.0/8**, **172.16.0.0/12**, **192.168.0.0/16** subnets as a filtering criterion.

7. If you have selected **Internal**, select the routing type (**Auto/Custom**).

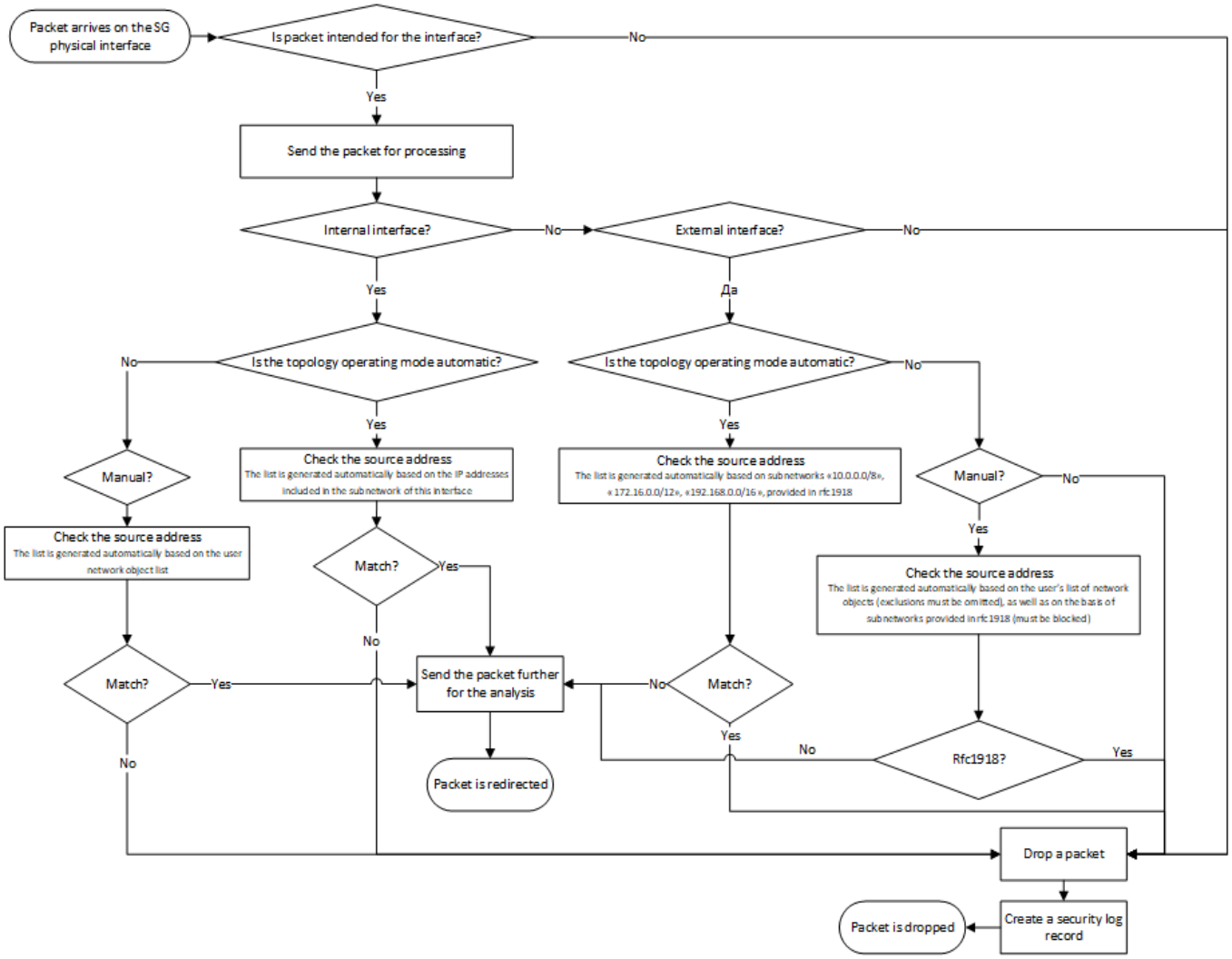
- If you select **Auto**, the topology for an internal interface is built automatically based on IP addresses included in this interface subnet.
- If you select **Custom**, the topology is built automatically based on the network objects user list. To do so, click and select network objects from the drop-down list.

8. Select the required dynamic routing protocol (**BGP** or **OSFP**), depending on the one that is in use.

Note.
In the **Allowed protocols** drop-down list, you can select the required parameters only if the dynamic routing mode is enabled on the Security Gateway.

Packet filtration depending on topology (anti-spoofing)

The packet filtering scheme depending on the topology (anti-spoofing) is shown in the figure below.



Configure bond

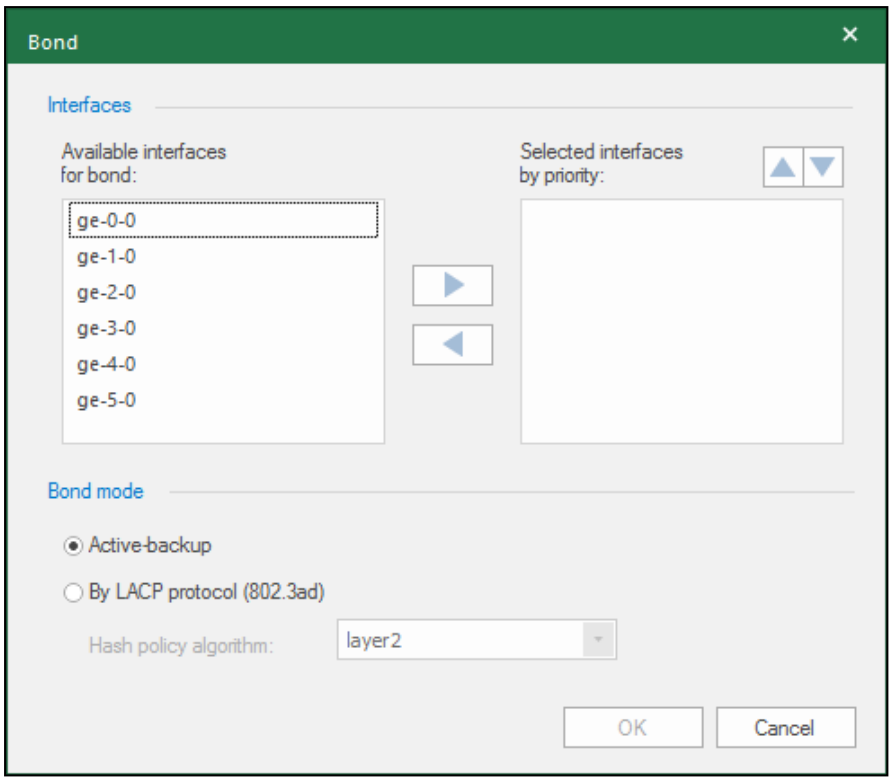
A bond is an aggregation of several physical channels into a logical one, which makes it possible to increase the throughput and reliability of a channel.

Attention!
You can configure bonds only after information about Security Gateway physical interfaces has appeared.

To configure a bond:

1. Go to **Structure**, select the required Security Gateway and click **Properties**.
   The respective dialog box appears.
2. On the right, select **Interfaces**.
   The list of interfaces appears.

3. On the right, click .
   The **Bond** dialog box appears.



4. Select the required interface on the left and click to move it to the bond.

Note.
VLAN is supported by all the bond modes (see [7]).

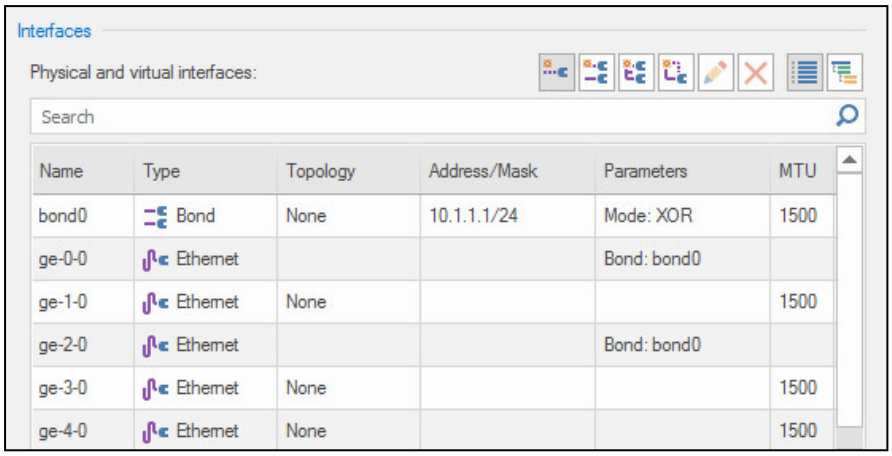
   The **ge-0-0** and **ge-2-0** interfaces are added.

5. Select the required interface on the right and click to exclude it from the bond.
6. Set the priority of bond interfaces by clicking and .
7. Select the bond mode. In case of selecting **LACP**, select the hash policy algorithm in the respective drop-down list. There are the following bond modes:

Mode	Description
Active backup	Traffic is passed through the interface with the lowest priority (active) while other interfaces are backup. If the active interface fails, the traffic will be automatically redirected to the operating backup interface with the highest priority. When you restore the active interface, the traffic will be automatically redirected back to it. This mode does not require any special configuration of devices to which aggregated interfaces are connected. This mode enables failover when other devices do not support LACP
By LACP protocol (802.3ad)	An interface is selected according to the selected hash policy: • layer2 (default); • layer2+3; • layer3+4. The respective configuration is required for devices of the aggregated channel

8. Click **OK**.

The created bond appears in the list with the inherited configurations of the bonded interfaces **ge-0-0** and **ge-2-0**.



9. Save the configuration and install the policy on the Security Gateways with the reconfigured parameters.

Note.
After creating a bond in the local menu, you can configure IP addresses of this bond in **Network interfaces** section in the local menu.

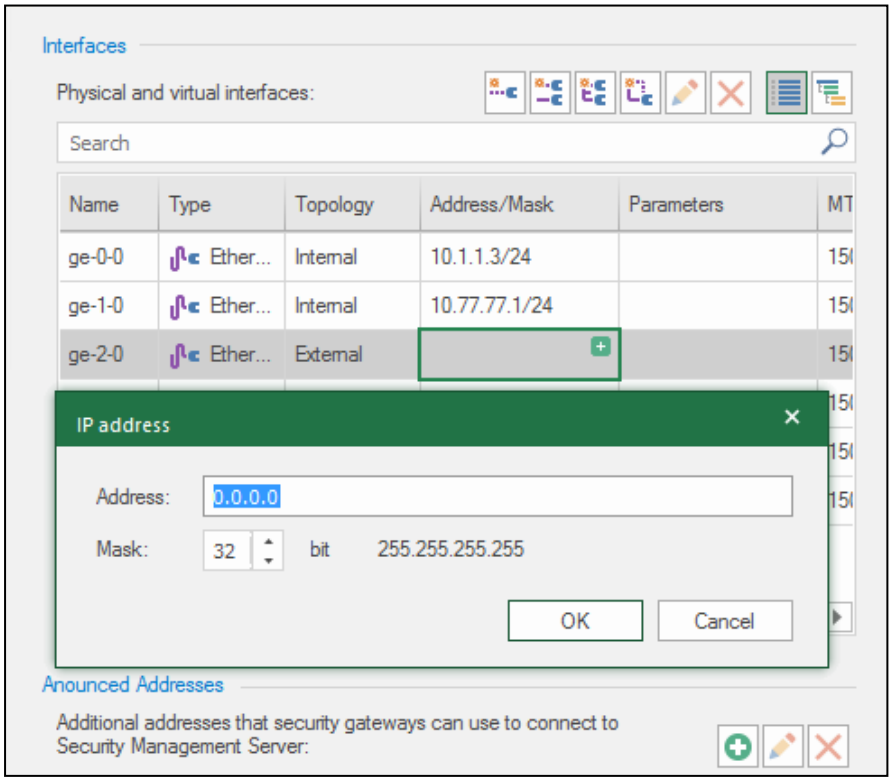
Configure IP address

To configure an IP address using the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties**.
   The respective dialog box appears.
2. On the right, select **Interfaces**.
   The list of interfaces appears.
3. In the required interface line, click  in the **Address/Mask** cell.

Note.
To edit an IP address, right-click the respective **Address/Mask** cell and select **Properties**.

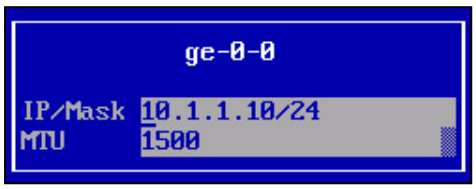
The respective dialog box appears.



4. Select the IP version by clicking the respective option buttons, enter the IP address and specify the mask.
5. After you have configured all the required parameters, save changes and install the policy on the Security Gateways with the reconfigured parameters.

To configure an IP address using the local menu:

1. In the main menu of the required Security Gateway, go to **Settings**, select **Network** and press <**Enter**>.
   The respective menu appears.
2. Go to **Network interfaces**, select the required interface and press <**Enter**>.
   The dialog box where you can configure network interface parameters appears.



3. Enter the IP address with the mask and the MTU value, then press **<Enter>**.
   You will be returned to **Network interfaces**. Select another interface and repeat steps **1** and **2** if necessary.
4. After you have finished configuring network interfaces, go back to **Settings**, select **Apply local policy** and press **<Enter>** to apply changes and save them in the Security Management Server database.
5. Confirm changes using the Security Management Server local menu or the Configuration Manager.

Configure DF bit

If an IP packet name contains the DF bit, further packet fragmentation via network equipment is forbidden.

In Continent, the DF bit can be reset for transit traffic on the outbound network interface.

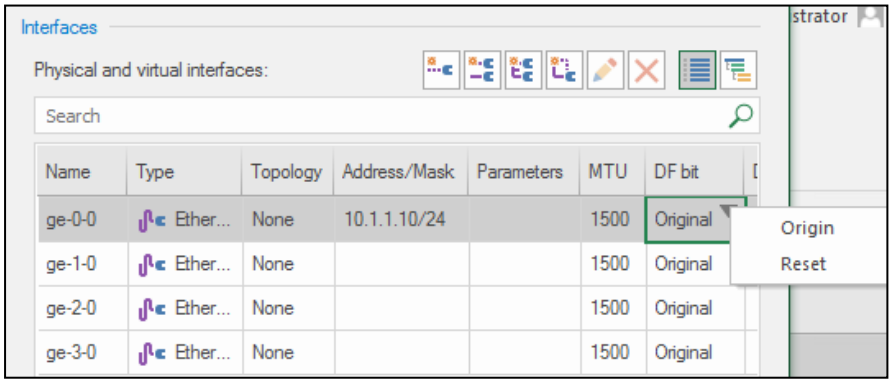
The **DF bit** parameter state is **Original** for every network interface by default.

To reset the DF bit in outbound packets, select **Reset** in the **DF bit** parameter of the selected interface.

Additional settings for packet fragmentation are not provided.

To configure the DF bit in the Configuration Manager:

1. In the **Interfaces** section, select an interface and click ▼ in the **DF bit** cell.
   The drop-down list appears.



2. Select **Origin** or **Reset**.
3. Click **OK**.
4. After configuring parameters, save the Security Management Server configuration and install the policy on the required Security Gateways.

Configure announced Security Management Server addresses

Announced Security Management Server addresses are IP addresses using which Security Gateways connect to the Security Management Server. This connection is performed if the main Security Management Server IP address is unavailable for some reason. For example, when the Security Management Server is behind the NAT.

Announced addresses are valid for all Security Gateways connected to the Security Management Server.

Note.
Announced Addresses are included in the configuration of each Security Gateway after a policy is installed. You do not need to additionally configure Security Gateways by the local management tools.

To configure Security Management Server announced addresses:

1. In the Configuration Manager, go to **Structure**, select the required Security Management Server and click **Properties** on the toolbar.

   The respective dialog box appears.
2. On the left, select **Interfaces**.

   The list of interfaces appears.
3. Click in the **Announced Addresses** parameter group, then specify the IP address or additional addresses. The Security Gateway can connect to the Security Management Server using these addresses.

4. Click **OK** to save the changes in the Security Management Server configuration.
5. Install the policy on the Security Management Server and all subordinate Security Gateways.

   Wait for the installation to be completed.

Configure additional addresses on the Security Gateway

Additional addresses of Security Gateways are IP addresses using which Security Gateways connect to the Security Management Server. This connection is performed if the main IP address of the Security Management Server is not available for the Security Gateway. For example, when the Security Management Server is behind the NAT.

The difference from announced addresses is that an announced address is configured on the Security Management Server and covers all subordinate Security Gateways, while an additional address is configured individually on a specific Security Gateway.

Additional addresses are configured in the Configuration Manager or by the local management tools.

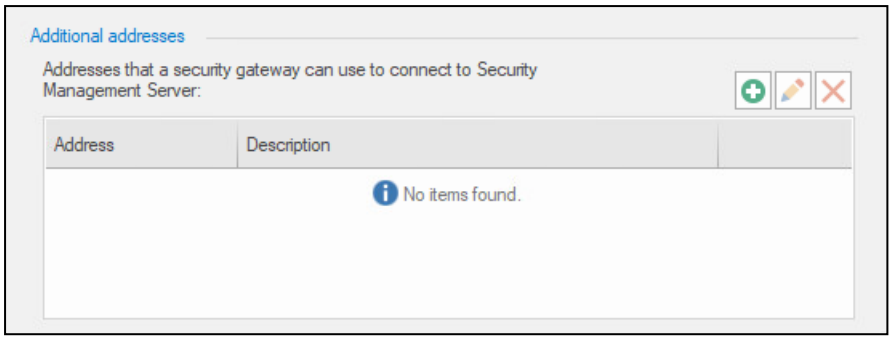
Note.
In the Security Gateway local menu, you cannot view or change the address of the Security Management Server to which it is connected.

To configure additional IP addresses in the Configuration Manager:

1. In the Configuration Manager, go to **Structure**, select the required Security Management Server and click **Properties** on the toolbar.

   The respective dialog box appears.
2. On the left, select **Interfaces**.

The list of interfaces appears.



3. Click in the **Announced Addresses** parameter group, then specify the IP address or additional addresses.
   The Security Gateway can connect to the Security Management Server using these addresses.
4. Click **OK** to save the changes.
5. Install the policy on the current Security Gateway.
   Wait for the installation to be completed.

To configure additional IP addresses using the local management tools:

1. In the main menu of the Security Gateway local management tools, select **Settings** and press **<Enter>**.
   The **Settings** menu appears on the screen.
2. Select **Network** and press **<Enter>**.
   The **Network** menu appears on the screen.
3. Select **Add Security Management Server address** and press **<Enter>**.
   The **Add Security Management Server address** menu appears on the screen.

4. Enter the Security Management Server IP address, specify port **6666** and press **<Enter>**.
   When the new IP address for connecting the Security Gateway to the Security Management Server is added, the success message appears.
5. Press **<Enter>** to return to the **Network** menu.
6. To apply the new parameters, return to the **Settings** menu, select **Apply local policy** and press **<Enter>**.
   Wait for the operation to complete.
7. Confirm the changes in the Security Management Server.

Change IP address of the Security Management Server interface

A secure Security Management Server IP change (without losing the connection between Security Management Server and the Security Gateway) is possible using announced addresses.

First, a new address is announced in the Security Management Server. Then, this address is assigned to the Security Management Server network interface.

To change the IP address of the Security Management Server management interface:

1. In the Configuration Manager, go to **Structure**, select the required Security Management Server and click **Properties** on the toolbar.
   The respective dialog box appears.
2. On the left, select **Interfaces**.

The list of interfaces appears.

3. Click in the **Announced Addresses** parameter group, then specify the IP address or additional addresses. The Security Gateway can connect to the Security Management Server using these addresses.

   Note.
   Announced addresses are included in the configuration of each Security Gateway after a policy is installed. You do not need to additionally configure Security Gateways by the local management tools.

4. Click **OK** to save the changes.
5. Install the policy on the Security Management Server and on all subordinate gateways.

   Wait for the policy installation task to be completed.

   The address will be added to Security Gateways and be used to connect to the Security Management Server.
6. Open the **Properties** dialog box again. Replace the IP address of the management interface with the address mentioned in step **3** and click **Apply**.

   Note.
   If you need to save the previous IP address, you can add a new IP address to any interface.

   Attention!
   Replacing the management interface IP address may lead to the necessity to make changes to the static route table. For this, select **Static routes** in the left part of the dialog box in the Security Gateway section and make the necessary changes.
7. Click **OK** and install the policy on the Security Management Server.

Note.
When the procedure is complete, create a full backup copy of the Security Management Server (see [**5**]).

VLAN interfaces

In Continent, you can work with VLANs. To use VLANs, you can create virtual interfaces.

Attention!
You can create and configure VLAN interfaces only after the Security Management Server has received information about physical interfaces.

VLAN interfaces are displayed in the list of Security Gateway interfaces alongside physical ones.

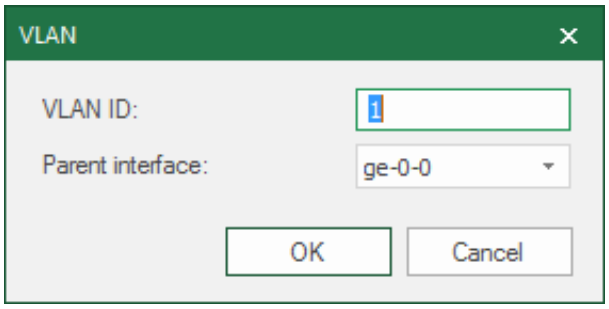
Create a VLAN interface

To create a VLAN interface:

1. Go to **Structure**, select a required Security Gateway in the list and click **Properties** on the toolbar.

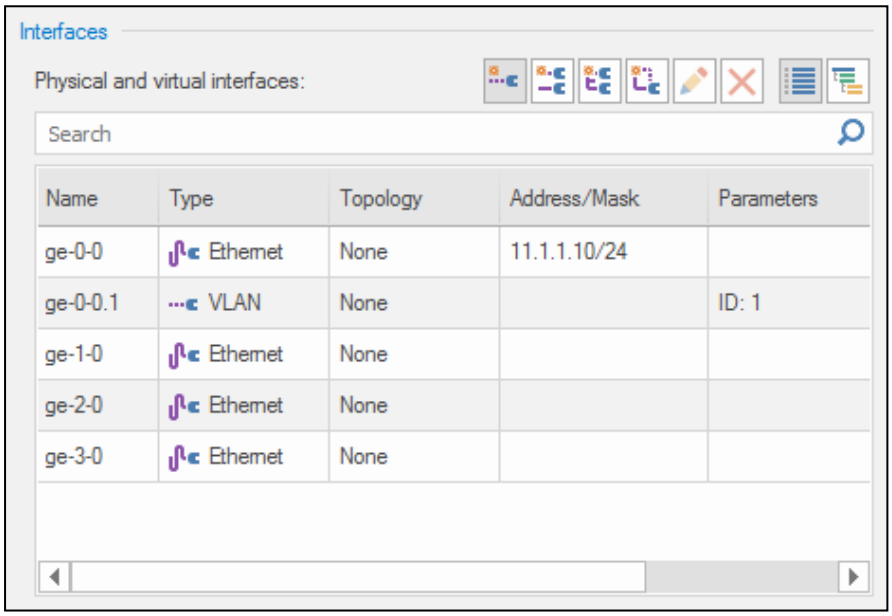
   The respective dialog box appears.
2. In the **Interfaces** section, select a physical interface required to be a parent one for a VLAN interface and click .

The dialog box with the parameters of a new VLAN interface appears.



The dialog box displays a VLAN ID assigned by default and the parent interface.

3. Change the VLAN ID and the parent interface, if necessary, and click **OK**.
   The created VLAN interface appears in the list.



4. Configure the other parameters: **Topology**, **Address/Mask**, **MTU** and **Description**.

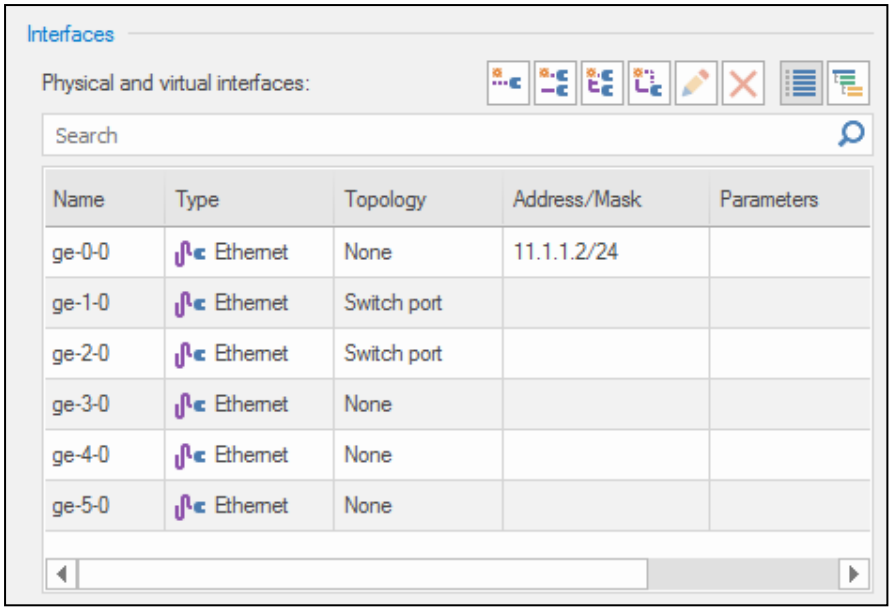
Attention!
The MTU on a VLAN interface can be changed only if its value on the parent interface is changed.

Bridge interfaces

You can combine Security Gateway interfaces into a bridge that you can also include in a virtual switch.
A bridge interface can contain no physical interfaces. It can also be used separately from a virtual switch.
You can assign an IP address to a bridge interface and use it to transfer data from L2VPN to L3VPN.
For more information on virtual switches used in L2VPN and bridge interface use examples, see [**3**].

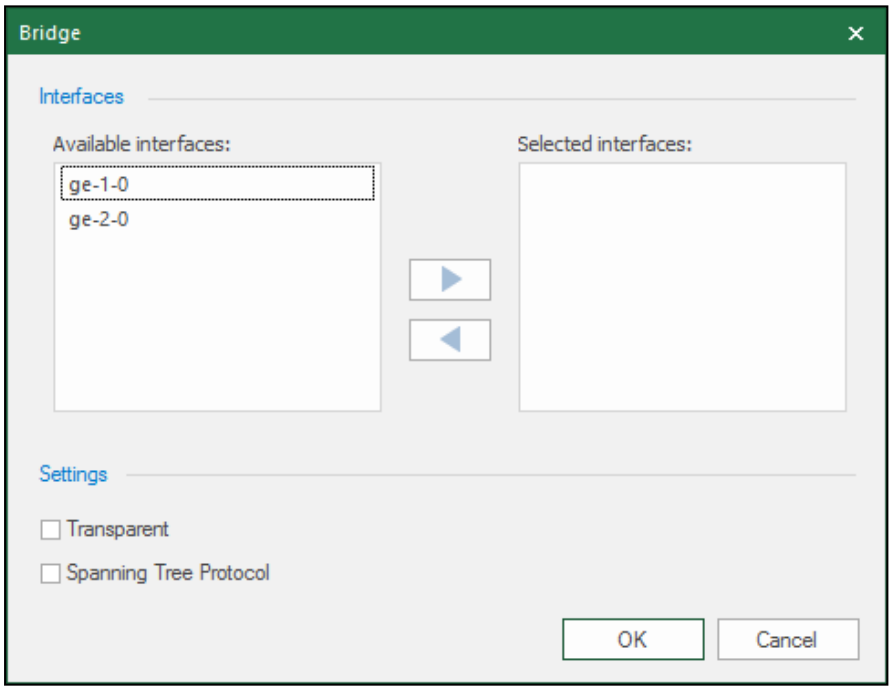
To create a bridge interface:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.
2. In the **Interfaces** section, set the **Switch port** topology for the interfaces to be included in the bridge interface (see p. **9**).



3. Click .

   The **Bridge** dialog box appears.



   On the left, you can see the interfaces of the **Switch port** topology.

4. To add an interface to the bridge, select it in the list of available interfaces and click .

   To remove an interface from the bridge, select it in the list of selected interfaces and click .

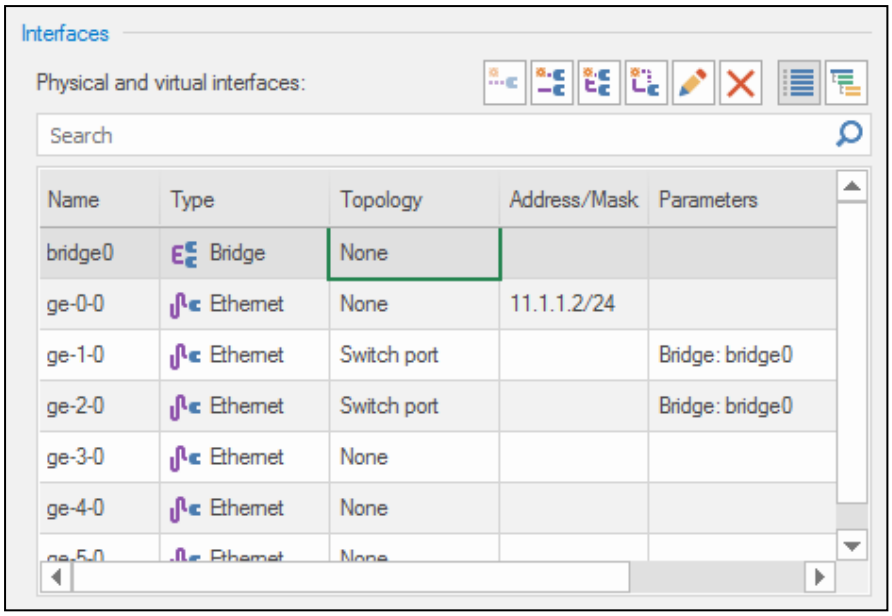
5. If you intend to use the bridge without including it to a virtual switch, select the mode you want it to operate in: **Transparent** or **Spanning Tree Protocol** (for more information on the modes, see [**3**]).

   Attention!
   If a bridge interface is used as part of a virtual switch, it inherits the operation mode from the virtual switch.

6. Click **OK**.

   The bridge interface appears in the list. The topology set by default is **None**.

In the **Parameters** column, you can see which interfaces are in use as bridge parts.



To delete a bridge interface:

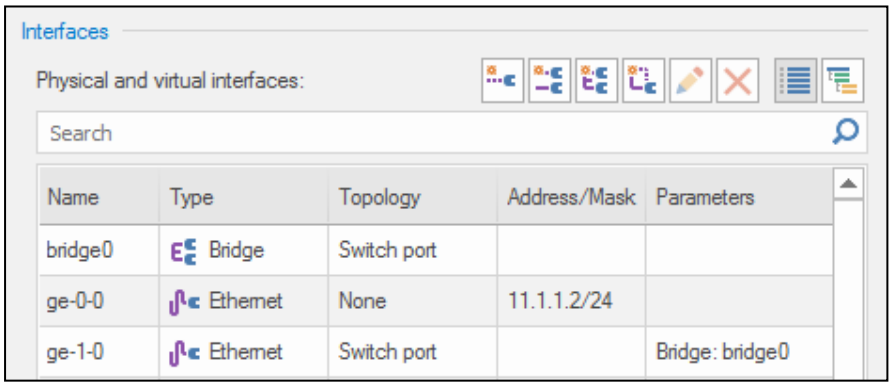
1. Select a bridge interface in the list and click .

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

   The selected bridge interface is deleted from the list.

To assign an IP address to a bridge interface:

1. For a bridge interface, specify the **Switch port** topology (see p. **9**).



2. Configure the IP address (see p. **13**) and click **OK**.

   The specified IP address appears in the list.
3. Save the configuration changes.

Loopback interfaces

The loopback interface configuration is performed using the Configuration Manager.

Attention!
You can create and configure loopback interfaces only after the Security Management Server has received information about physical interfaces.

To configure a loopback interface:

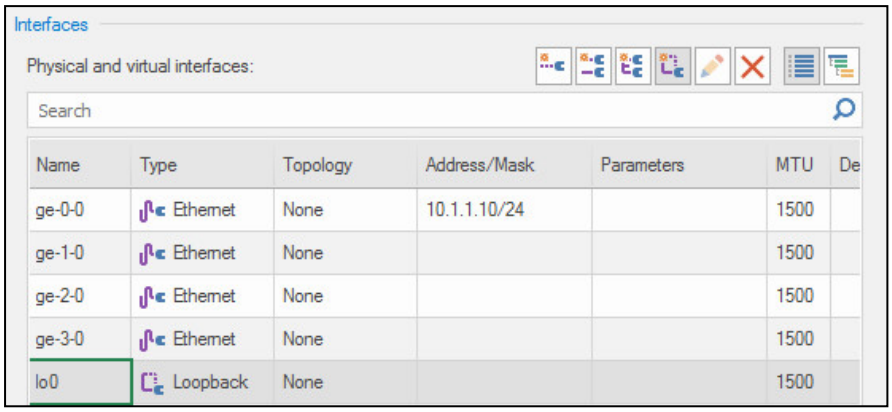
1. In the Configuration Manager, go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.

   The respective dialog box appears.
2. On the left, go to **Interfaces**.

The list of interfaces appears on the right.

3. Click .

   A loopback interface appears on the list.

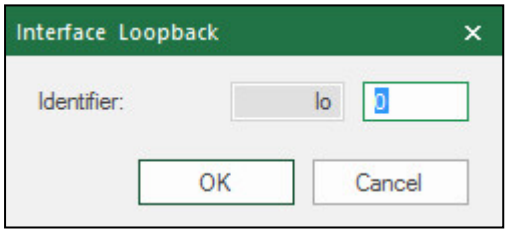


   By default, it is assigned the **0** sequence number.

Note.
When you add a new loopback interface, it is assigned a number next to the last one. You can change a number in the **Name** cell.

4. If you need to change the sequence number, click in the **Name** column.

   The **Interface Loopback** dialog box appears.

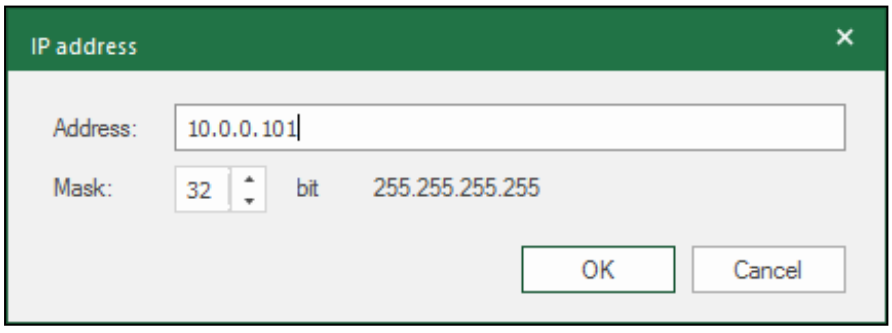


5. In the **Identifier** field, enter a new sequence number and click **OK**.

   The sequence number is changed.

6. In the **Address/Mask** column, click .

   The respective dialog box appears.



Note.
You can use only the **32** mask.

7. Enter the IP address and the mask, then click **OK**.

   The dialog box is closed and the address with the mask of the loopback interface appears in the list.

8. Change MTU and enter a description in the respective fields if necessary.
9. If you need to use other loopback interfaces according to the topology, take steps **3**–**7** to add them to the list.

Rename network interfaces of custom platforms

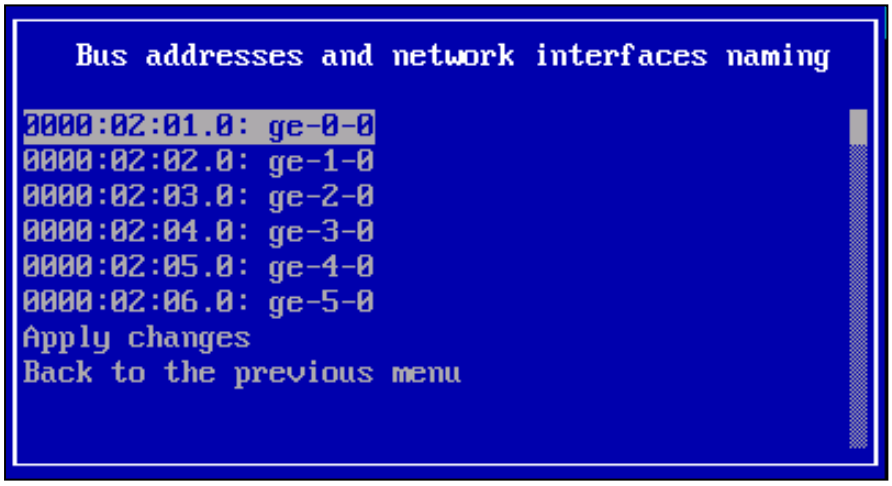
Continent allows you to rename original network interfaces of custom platforms using the local menu.

You can change a name before Security Management Server configuration or before connecting a Security Gateway to the Security Management Server.

To rename interfaces:

1. In the local menu, select **Settings** and press **<Enter>**.
   The **Settings** menu appears.

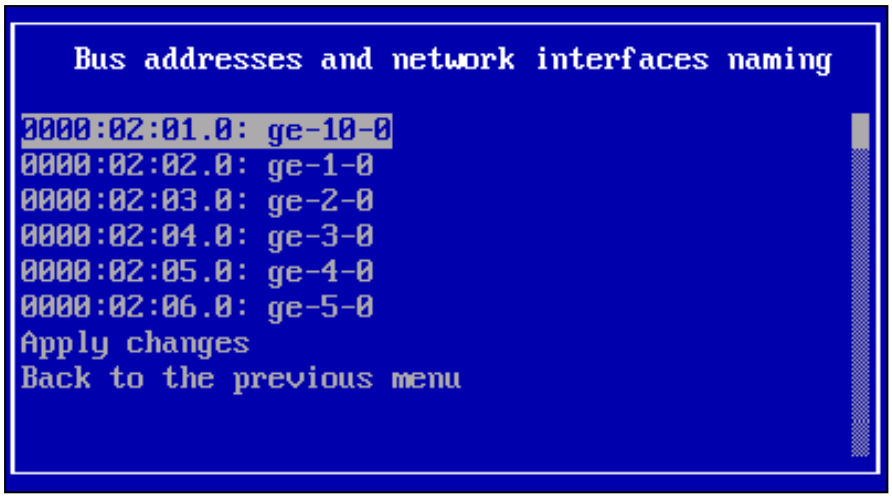
2. Select **Network interfaces naming** and press **<Enter>**.
   The **Bus addresses and network interfaces naming** menu appears.



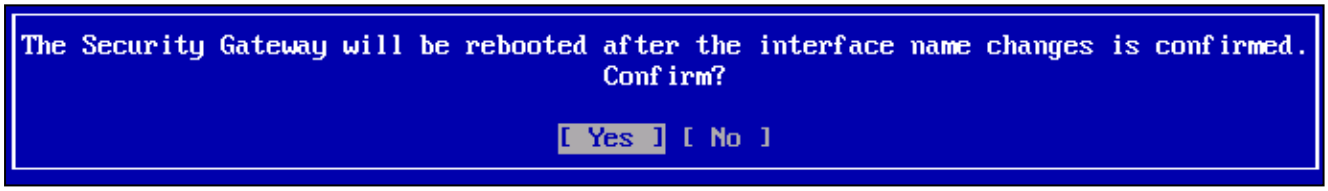
3. Select the required interface and press **<Enter>**.
   The **Renaming a network interface** dialog box appears.

4. Enter a new interface name and press **<Enter>**.

You will be returned to the previous menu where the new interface name will be displayed.



5. If necessary, perform steps **3** and **4** to rename other interfaces.
6. In the **Bus addresses and network interfaces naming** menu, select **Apply changes** and press **<Enter>**.
   The dialog box prompting you to apply changes appears.



7. Select **Yes** and press **<Enter>**.
   The Security Gateway reboot starts.

Multi-WAN

The following settings allow you to configure a network when connecting the Security Gateway to several external networks simultaneously. There are the following Multi-WAN modes:

- transfer of traffic according to the routing table;
- ensuring failover for a communication channel (backup);
- traffic balancing between external interfaces of a Security Gateway.

Attention!
Multi-WAN operation on Security Gateways with the Security Management Server and the standby Security Management Server is not supported.

Only traffic sent to the network interface of a Security Gateway with **Internal** topology goes to Multi-WAN.

In Multi-WAN, outgoing traffic is distributed between WAN channels according to WAN rules created by the administrator.

ICMP outgoing packets do not reach the Multi-WAN, but are processed according to the static routes of the main routing table.

The following types of traffic must not reach the Multi-WAN:

- outgoing ICMP packets;
- traffic of the synchronization network in a security cluster;
- management and logging traffic (Security Gateway — Security Management Server);
- traffic from the Security Gateway towards all required hosts (including the Security Management Server and the standby Security Management Server) located in the network behind its internal interface;
- traffic between all networks passing through its interfaces with **Internal** topology and not intended for passing to the WAN channels.

To ensure that packets of the traffic types mentioned before do not enter the WAN channels, but are processed according to the routing table, the administrator must create respective exclusion rules.

When you install the policy on the Security Gateway, traffic flow is interrupted. To minimize the interruption time, we recommend you configure the default route in the routing table.

Multi-WAN configuration includes:

- enabling Multi-WAN mode and specifying the main parameters;
- configuring WAN channels;
- creating WAN rules;
- installing a policy on the Security Gateway.

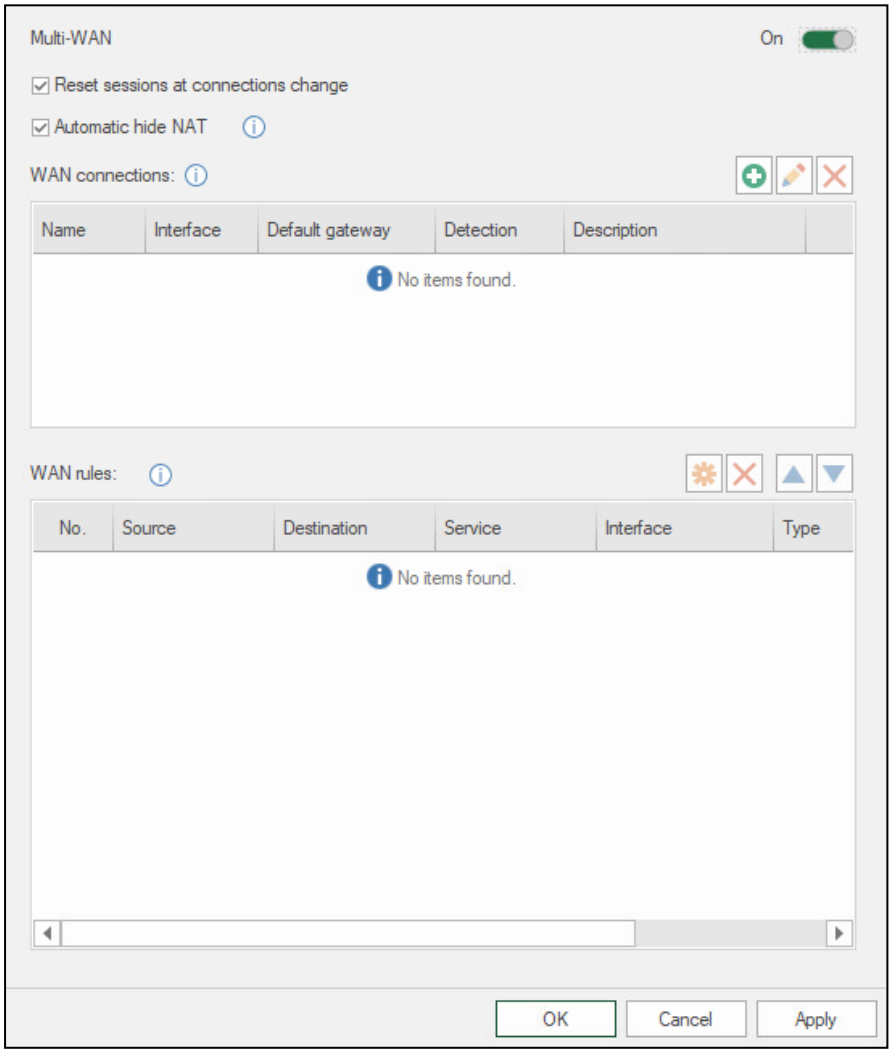
When Multi-WAN is in operation, you must use internal NTP and DNS servers.

You can configure modes and channels in Multi-WAN in Security Gateway properties.

Enable Multi-WAN

To enable and configure Multi-WAN:

1. Select the Security Gateway you need to configure and click **Properties** on the toolbar.
   The Security Gateway properties dialog box appears.
2. On the left, select **Multi-WAN**.
   The Multi-WAN settings appear on the right.



   If Multi-WAN has not been configured earlier or is turned off, settings are unavailable.
3. Turn on the toggle in the upper-right corner.
   Multi-WAN parameters are available for editing now.
4. Specify the general Multi-WAN parameters, select or clear the respective checkboxes.

Parameter	Description
Reset connections at channel change	Allows you to turn on/off resetting of current connections when switching to another channel
Automatic hide NAT	Allows you to turn on/off automatic creation of hide NAT rules

Attention!

The translation is done for all traffic that falls into the Multi-WAN and does not fall into an exception. In this case:

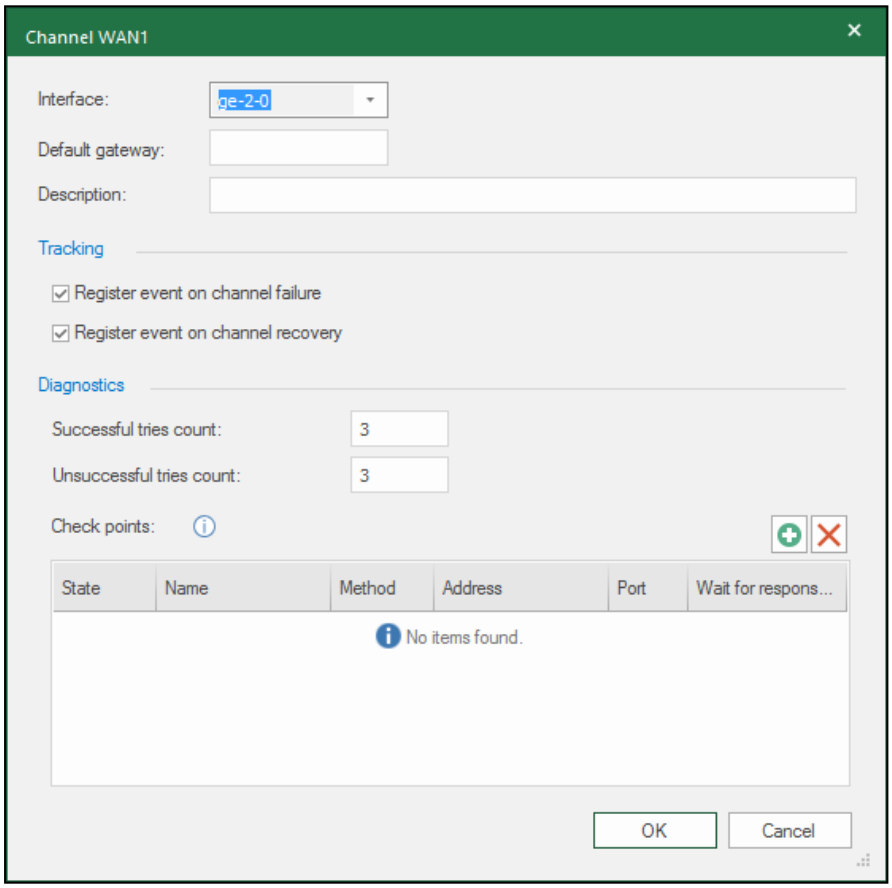
- for traffic coming to the SECURITY CODE LLC external interface and coming from the internal interface, the source address is swapped with the WAN interface address in the packet that the Security Gateway sends from the internal interface;
- for traffic coming to the SECURITY CODE LLC external interface and falling under the recipient NAT rules formed in the access control, the source address is swapped with the WAN interface address in the packet that the SECURITY CODE LLC sends from the internal interface.

Configure WAN channels

To configure channels:

1. To create WAN channels, click  .

   The WAN channel configuration dialog box appears.



2. Specify the Security Gateway external interface on which the WAN channel should be configured.

   The first free external interface is offered automatically.

3. To specify another interface, select it in the **Interface** drop-down list.

Attention!

You can use only physical interfaces as an external interface for a WAN channel, as well as VLAN interfaces based on them. You cannot use bond interfaces and objects based on them for WAN channels.

4. In the **Default gateway** text box, specify the IP address of the provider's gateway, which is next to the Continent Security Gateway. In the **Description** text box, enter a short description of the WAN channel.
5. Specify the tracking parameters.

Parameter	Description
Register event on channel failure	Allows you to enable/disable an event registration on channel failure
Register event on channel recovery	Allows you to enable/disable an event registration on channel recovery

6. Specify the diagnostics parameters.

Parameter	Description
Successful tries count	The number of successful tries to determine the recovery of a WAN channel. Maximum value – **10**
Unsuccessful tries count	The number of unsuccessful tries to determine the failure of a WAN channel. Maximum value – **10**

7. To create a check point (IP address or domain name), click  . Using this check point, Continent checks WAN channel availability.

   Default check point parameters appear.

8. Specify the values of check point parameters.

Parameter	Description
State	On/Off
Name	Mnemonic indication of the check point
Method	Check point testing method: **ICMP** (ping) or **TCP** (connection handshake)
Address	The check point address for accessibility testing in the form of an IP address or domain name
Port	The check point port number as destination for TCP accessibility testing
Wait for response	Timeout of a response from the check point during accessibility testing with the specified method (ms). Maximum value – **3,000**

9. Add a second check point if necessary. The maximum number of check points is **2**.

Attention!

- If no check points have been created after WAN configuration, the Security Gateway will enable an implicit check point and send ICMP requests to the next node. If the administrator configures the first explicit check point, the implicit one will be disabled.
- The channel will be considered inoperable if all enabled checkpoints fail.
- If the next node of the WAN channel has ICMP Reply disabled, you need to configure at least one check point which will be used for the diagnostics of this channel. Without this check point, the channel will be considered inoperable.

10. Click **OK**.

    The WAN channel configuration dialog box is closed and the created WAN channel appears in the **Interfaces WAN** list.

11. Repeat steps **1**–**9** for other WAN channels. The maximum number of WAN channels is **7**.

To edit WAN channel parameters:

- select the required WAN channel in the **Interfaces WAN** list, click  and edit the required parameters.

To delete a WAN channel:

- select the required WAN channel in the **Interfaces WAN** list and click .

Create WAN rules

When working with WAN rules, note the following:

- You cannot use the following Security Management Server objects in WAN rules:
  - users;
  - protocols and applications;
  - countries;

- DNS names;
- time intervals;
- QoS classes;
- Security Gateways different from Security Gateways on which Multi-WAN is configured.

- For each WAN transit rule, a duplicate rule for local traffic is created automatically, in which a network interface with the **Internal** topology and source addresses are dropped. If the created transit rule has only one address specified, the source will be **Any** in local traffic. In order for local traffic not to go to Multi-WAN, you must create an exclusion rule in which the source must be **Any**.

Attention!

When using WAN rules with the **Any** source and destination, you must create exclusion WAN rules for traffic:

- of a synchronization network if a security cluster is used;
- from the Security Gateway in the direction of all required hosts (including Security Management Server and stand-by Security Management Servers) if they are located within a network outside its internal network interface;
- between all Security Gateway networks, passing through its network interfaces with the **Internal** topology and for which sending into WAN channels is not required.

Traffic that meets rules of the **Exclusion** type is processed according to the configured static routes of the routing table. These rules with the **Exclusion** type must be at the top of the WAN rule list. You can find an example of configuring such rules on p. **30**.

The rules are created by the administrator after enabling Multi-WAN and configuring the channels.

By default, the list of rules is empty.

To create a list of rules:

1. On the Multi-WAN settings tab, in **WAN rules**, click  .

   A new rule with default parameters appears in the list.

   If the list already contains rules created earlier, a new rule will be added to the end of the list with a respective sequence number.

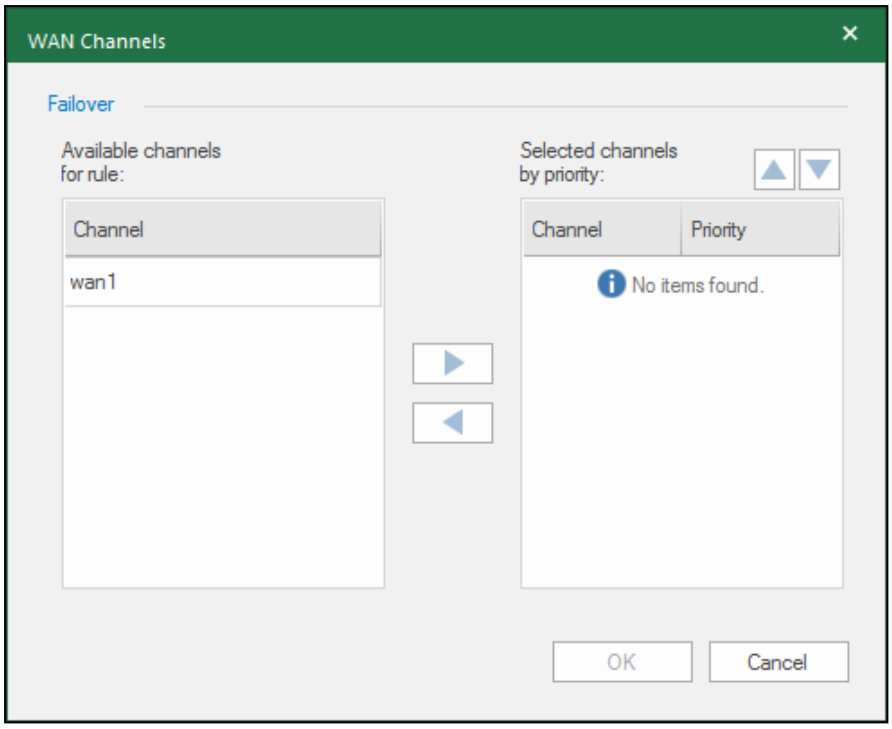
2. Edit the required rule parameters if necessary:
   - To change a parameter value, click the pop-up button on the right of the value. Select a parameter value from the list. If the required parameter value is missing, you can add it to the list.
   - If you need to restore the parameter to its default value, select and delete it.

Parameter	Description
№	Sequence number of a rule in the list
Source	A network object or a list of network objects. You can select it from the list of available network objects. The default value is **Any**
Destination	A network object or a list of network objects. You can select it from the list of available network objects. The default value is **Any**
Service	A service or a list of services. You can select it from the list of available services. The default value is **Any**
Out Interface	A list of determined physical interfaces of a Security Gateway with the Internal topology, which are used as inbound for network traffic. If the **Automatic** value is specified, the system will independently select the interface to which this rule will be bound based on the topology and addressing scheme
Type	Multi-WAN modes: • **Failover**; • **Balancing**; • **Exclude**
Channel	A list of WAN channels used for the **Failover** and **Balancing** modes (see below)

   - If the **Type** parameter is set to **Exclude**, traffic will be transmitted according to the routing table. In this case, you cannot choose WAN channels in the **Channel** parameter. Go to step **9**.
   - If the **Type** parameter is set to **Failover**, go to step **3**.
   - If the **Type** parameter is set to **Balancing**, go to step **6**.

3. Set priority levels to WAN channels. To do so, click the button on the right of the **Channel** cell.

The **WAN Channels** dialog box appears.



The list on the left contains all available WAN channels, the list on the right is designed for configuring the channel priority.

4. Move channels which should be assigned priority from the left list to the right one by one.

Note.
You can select several channels from the left list and move them to the right list simultaneously.

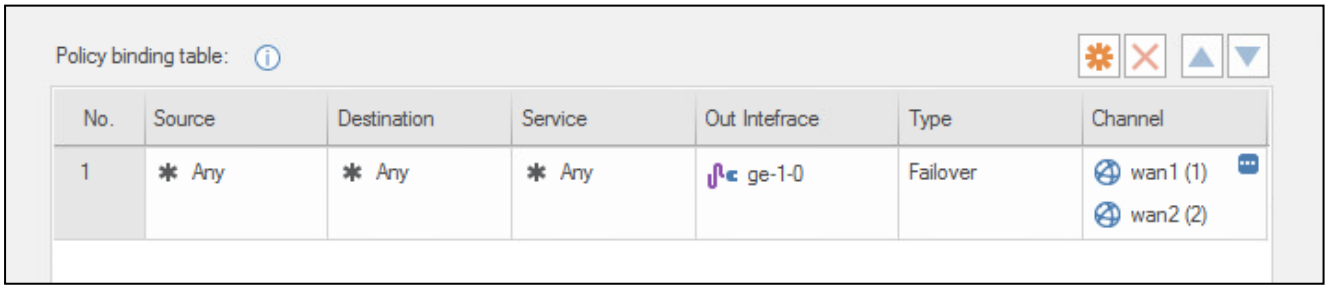
When you move a channel to the right list for the first time, it is automatically assigned the highest priority level — **1**. The next channel is assigned the following priority level in descending order — **2**, **3**, etc.

To change priority level, select a channel in the right list and click ▲ and ▼.

Attention!
The minimum number of channels with the **Failover** type is **2**.

5. Click **OK**.

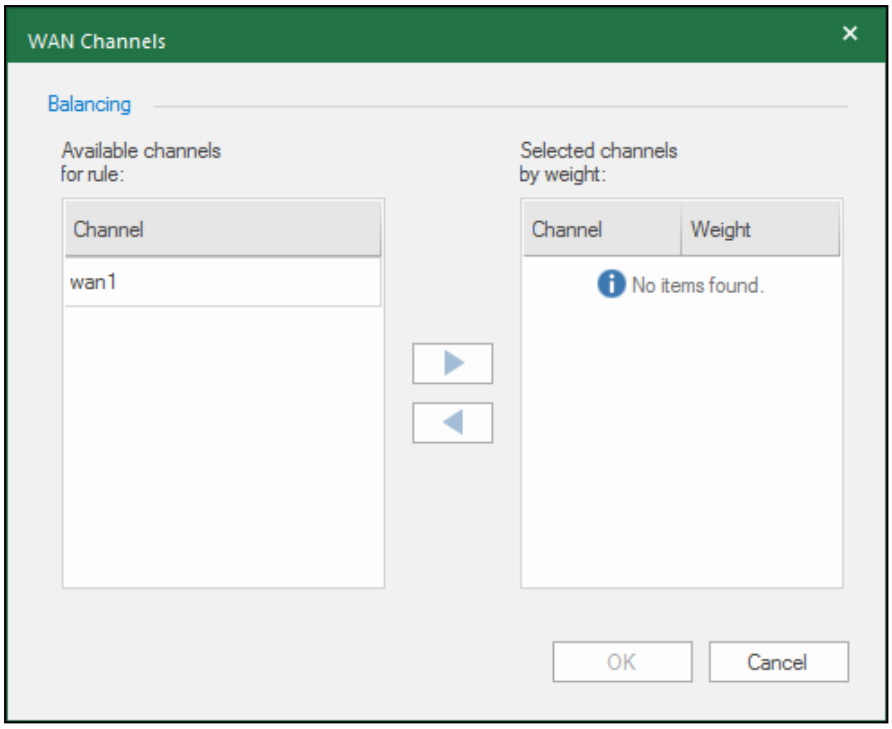
The **WAN Channels** dialog box is closed and the created rule with WAN channels and their respective priorities appears in the list.



Go to step **9**.

6. Specify the channel weight. To do so, click the button on the right of the **Channel** cell.

The **WAN Channels** dialog box appears.



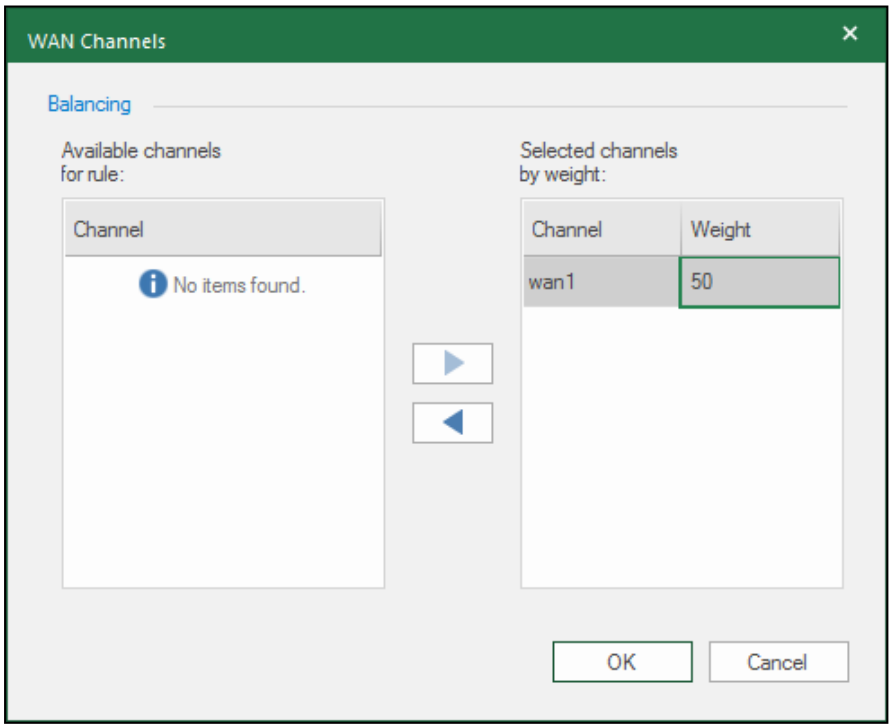
The list on the left contains all available WAN channels, the list on the right — channel weights.

7. Move channels which should be assigned weight from the left list to the right one by one.

Note.
You can select several channels from the left list and move them to the right list simultaneously.

When you move channels to the right list, they are automatically assigned a weight of **1**.

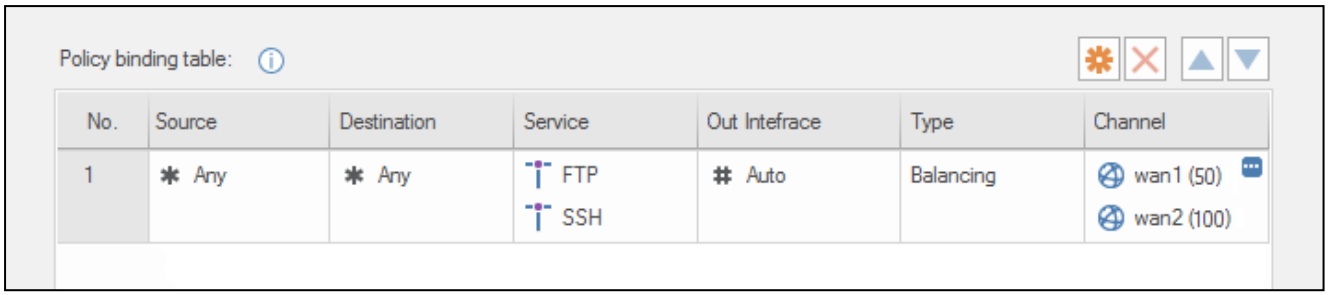
Specify channel weights in the right list. The maximum weight value is **100**.



Attention!
The minimum number of channels with the **Balancing** type is **2**.

8. Click **OK**.

The **WAN Channels** dialog box is closed and the created rule with WAN channels and their assigned weights appears in the list.



9. Add all required rules to the list (see steps **1**–**8**). The maximum number of WAN rules is **128**.

   To specify a rule intended only for local Security Gateway traffic, you must create an object of the host type with the address of any of the Security Gateway interfaces and specify it as the source.

   Note.
   Local traffic is traffic created directly by the Security Gateway.

   Rules for local Security Gateway traffic must be located at the top of the list of rules.

10. Configure the order of rule application if necessary.

    The rules are applied in the same order in which they are displayed in the list, starting from the first one.

    To change the application order, select the rule and move it up or down using the respective buttons.

    Attention!
    When using general WAN rules with the **Any** value as the source and destination, it is important to remember to create rules with the **Exclusion** type for traffic:
    - of synchronization network when using a cluster;
    - from the Security Gateway towards all required hosts (including the Security Management Server) located in the network behind its internal interface;
    - between all Security Gateway networks passing through its interfaces with the Internal topology and not requiring sending to WAN channels.

11. After configuring the list of rules, click **Apply** at the bottom of the **WAN Channels** dialog box, save the configuration and install the policy on the Security Gateway.

You can edit the list of rules using the following operations:

- add a new rule to the list;
- delete a rule;
- configure rule parameters;
- change the order of the rules in the list.

To perform these operations, use the respective buttons.

Attention!
For traffic that falls into a Multi-WAN rule with a **Failover** or **Balancing** type, the configured NAT rules will be ignored.

Example of Exclusion rule configuration

This subsection provides settings for WAN rules with the **Exclusion** type in the cluster.

The cluster has two WAN channels configured: **wan1** and **wan2**.

The Security Management Server IP address is **172.16.0.2**.

The cluster synchronization network is **192.168.1.0/30**.

It is necessary to create rules that exclude the redirection of control and logging traffic between the Security Gateway and the Security Management Server to the WAN channels, as well as traffic intended for synchronization of the main and backup gateways of the cluster.

Rules are created according to the description of the procedure for creating a list of rules (see p. **26**).

For a rule that excludes the direction of control and logging traffic to WAN channels, you need to create two Security Management Server objects of service type, in this example — Log_CUS and Management.

Log_CUS service parameters:

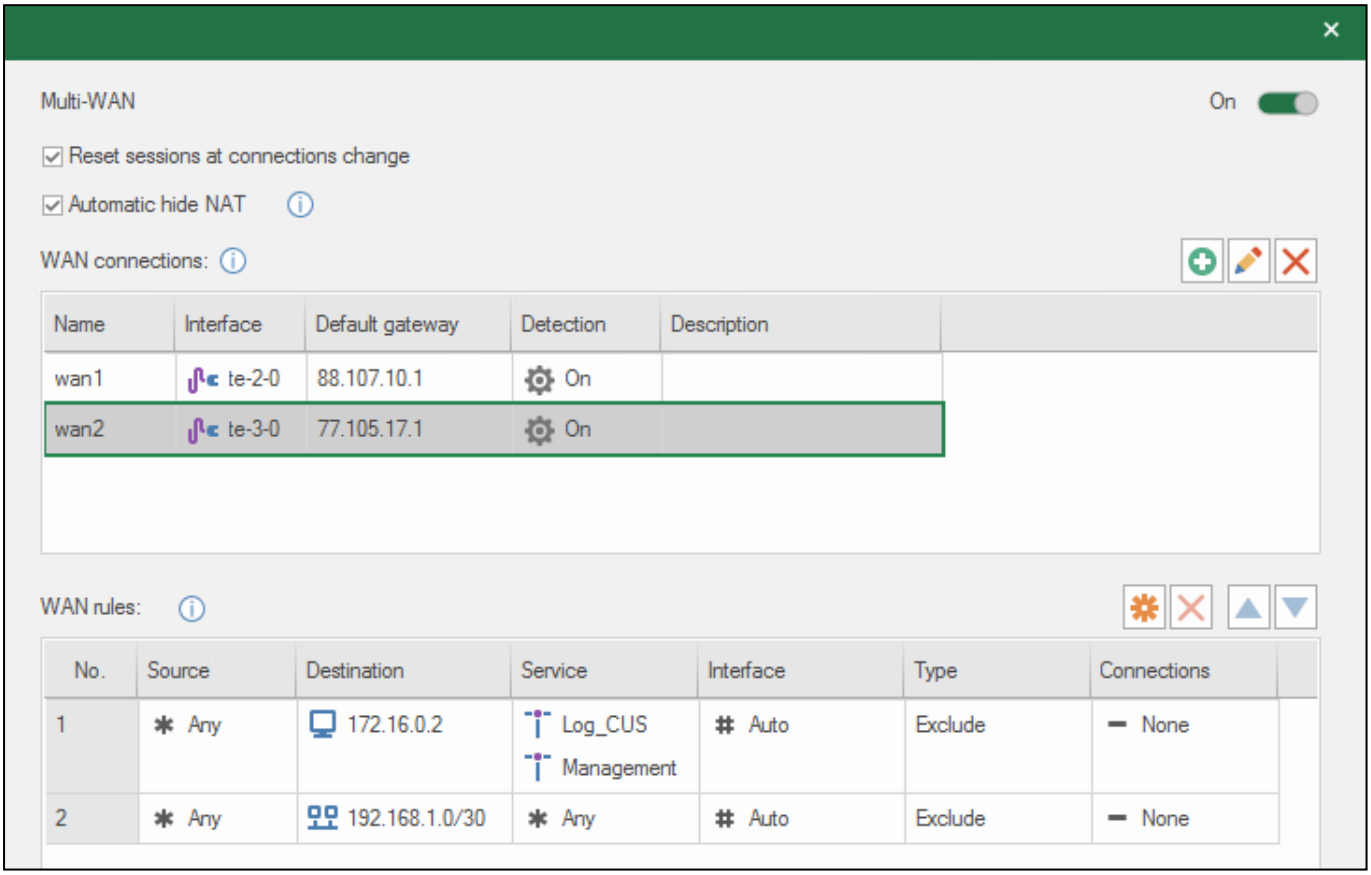
- protocol — **TCP**;

- destination port — **6666**;
- source port — **any**.

Management service parameters:

- protocol — **TCP**;
- destination port — **8888**;
- source port — **any**.

You can see the rules in the figure below.



The first rule allows you to avoid forwarding control and logging traffic between the Security Gateway and the Security Management Server to the WAN channels.

The second rule allows you to avoid forwarding traffic intended for the synchronization of cluster hosts to the WAN channels.

Example of resource publishing in Multi-WAN

This subsection provides an example of Multi-WAN settings for publishing a resource (for example, an FTP server) using an IP address of two different providers.

1. Choose the security gateway, on which you should configure settings, and go to the Multi-WAN settings section (see p. **24**).
2. Set general Multi-WAN parameters by clearing the **Automatic hide NAT** check box.
3. Set WAN channels (see p. **25**). In this example, these are channels wan1 and wan2.

Name	Interface	Next gateway	Diagnostics
wan1	ge-4-0	5.5.15.1	Turn on
wan2	ge-5-0	6.6.115.1	Turn on

Note.
The interface names and IP addresses of the following gateways are given as an example.

4. Set three WAN rules (see p. 26).

№	Source	Destination	Service	Interface	Type	Channel
1	10.10.10.1	10.0.0.0/8	Any	Automatically	Exclude	No
2	Any	10.0.14.168	management_1 management_2	Automatically	Exclude	No
3	10.0.0.0/8	Any	Any	Automatically	Balancing	wan1 (1) wan2 (1)

The rules first specify Excludes that should not be under control of Multi-WAN. For example, control traffic.

Rule №3 must have a private network as a source (in this example — **net_10.0.0.0/8**).

5. Create source and destination NAT rules for accessing the published resource and responses from it, depending on the interface used (for more information on translation rules, see [**3**]).

Rules example:

Source packet			Translated packet				Interface
Source	Destination	Service	Translation	Source	Destination	Service	
Any	5.5.15.10	FTP	Destination	Original	10.0.14.179	Original	ge-4-0
Any	6.6.115.10	FTP	Destination	Original	10.0.14.179	Original	ge-5-0
10.0.0.0/8	Any	Any	Source	5.5.15.10	Original	Original	ge-4-0
10.0.0.0/8	Any	Any	Source	6.6.115.10	Original	Original	ge-5-0

The first two rules are used for external access to the published resource via addresses of different providers.

The second two rules are the rules for outgoing NAT traffic from the internal network, including responses from the resource with adjustment for the outgoing interface. The source is the private network **net_10.0.0.0_8**.

6. Create the respective firewall rules (for more information on filtering rules, see [**3**]).
7. Save the changes and install the policy.

Routing parameters

This section describes how to configure routing settings when the Security Gateway is not in virtual routing mode. For virtual routing mode and related settings, see p. 42.

Security Gateways can work in both static and dynamic routing mode.

To work in static routing mode, the administrator must create static routes in the Configuration Manager or by means of the Security Gateway local menu. When the policy is applied, static routes are saved in the routing table. If virtual routing is used on the Security Gateway, each VRF zone has its own routing table with static routes.

Dynamic routing on the Security Gateway is implemented using the BIRD service. The administrator must create a configuration file and upload it to the Security Management Server database.

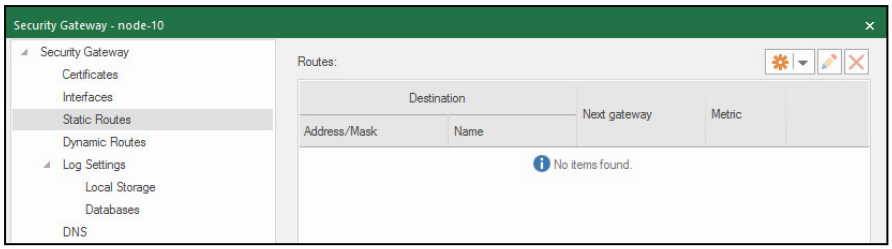
Static routing

You can create static routes using the Security Management Server and Security Gateway local menu.

To create a static route using the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
2. On the left, select **Static Routes**. In the right part of the dialog box, you will see a list of static routes.

If no static routes have been added, the list will be empty.



In a routing table, each line corresponds to one route. Further, you can see the list of fields and their descriptions.

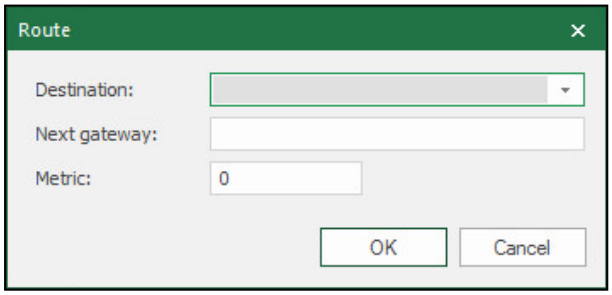
Parameter	Description
Address/Mask (Destination)	IP address and mask of a network object
Name	Name of a destination network object or the default route name
Next gateway	IP address of a gateway through which IP packets of the route should pass
Metric	Route priority used if there are several routes for the same value specified in the **Address/Mask** field

In case of planned changes of network settings, it is enough to edit them in advance in the routing table (see p. **34**). If changes were unplanned, you must also locally update the default gateway IP address on the Security Gateway (see p. **34**).

In the event of planned changes of the endpoint network device parameters, change them in the routing table (see p. **34**) in advance. If you have unplanned changes, you need to update the IP address of the default gateway using the local menu of a Security Gateway (see p. **34**).

3. To add a new static route to a Security Management Server network object (see [**3**]), click next to the route creation button and select **Network object** as in the figure below.

The **Route** dialog box appears.



4. Select a Security Management Server network object in **Destination**, in **Next gateway** — the next gateway in the route, in **Metric** — the required metric.

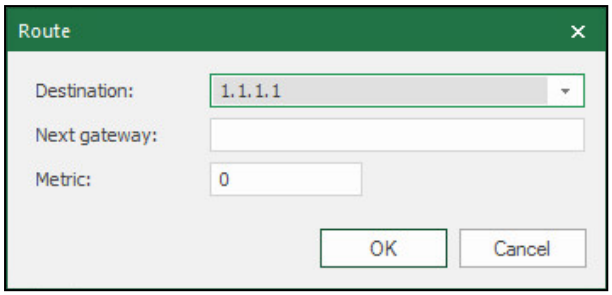
Note.
For the same network object, you can create several routes, in each of them you can specify their own next gateway. If the specified next gateway is not available in a route, the next route will be chosen. Using metrics, you can define the priority of each route. The larger the metric value is, the less priority the route has. The route with the highest priority has a metric value of 0.

5. Click **OK**.

The new route appears in the list.

6. To add a new route to an unregistered network object, click .

The **Route** dialog box appears.



7. Specify the IP address of a destination object, the next gateway in the route and the required metric (see the note above). Click **OK**.

   The new route appears in the list.

8. Add required static routes as described above.

   You can edit and delete static routes. To edit or delete them, select the required one and click or .

9. After you have finished configuring all the parameters, save the changes and install the policy on the Security Gateways with the reconfigured parameters. After the policy is installed, the specified static routes are added to the routing table corresponding to the VRF zone with ID 0 (for more information on VRF zones, see p. **42**).

To configure the routing table using the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
2. On the left, select **Static Routes**.
3. To edit a route, select it in the table, click , then make the required changes and click **OK**.
4. To delete a route from the routing table, select it in the table and click .
5. After you have finished configuring all the parameters, save changes and install the policy on the required Security Gateways.

To configure static routes using the local menu:

1. In the main menu, select **Settings** and press <**Enter**>.

   The **Settings** menu appears.

2. Select **Network** and press **<Enter>**.

   The network settings of the Security Gateway appear.

3. Select **Static routes** and press **<Enter>**.

   The list of static routes appears. The list contains the **IP or subnet**, **Gateway** and **Metric** fields.

4. To create a new route, press **<N>**.

> **Note.**
> To edit the existing route, select it in the list and press **<Enter>**, to delete — press **<Del>**.

The **New route** dialog box appears.

5. Enter the IP address of a remote network object, specify a gateway through which you can access the selected object, the metric and press **<Enter>**.

   If the specified gateway is accessible, a new route will be created and you will be returned to the **Static routes** list. If you need to add more routes, repeat steps **4** and **5**.

6. To apply changes, go back to **Settings**, select **Apply local policy** and press **<Enter>**.

> **Note.**
> If you have changed the local configuration, you can apply a local policy only once after making all the changes.

7. Wait for the operation to finish and confirm the changes locally on the Security Management Server or via the Configuration Manager tools.

Dynamic routing

Continent supports the following versions of dynamic routing protocols:

- OSPF — version 2;
- BGP — version 4.

The protocol support is based on BIRD (Internet Routing Daemon).

To enable dynamic routing, you need to create a BIRD configuration file. To do so, you can use any text editor or the built-in routing configuration editor in the Security Gateway properties.

Then, you need to upload the configuration file to the Security Management Server using the Configuration Manager and send it to the Security Gateway by installing the policy.

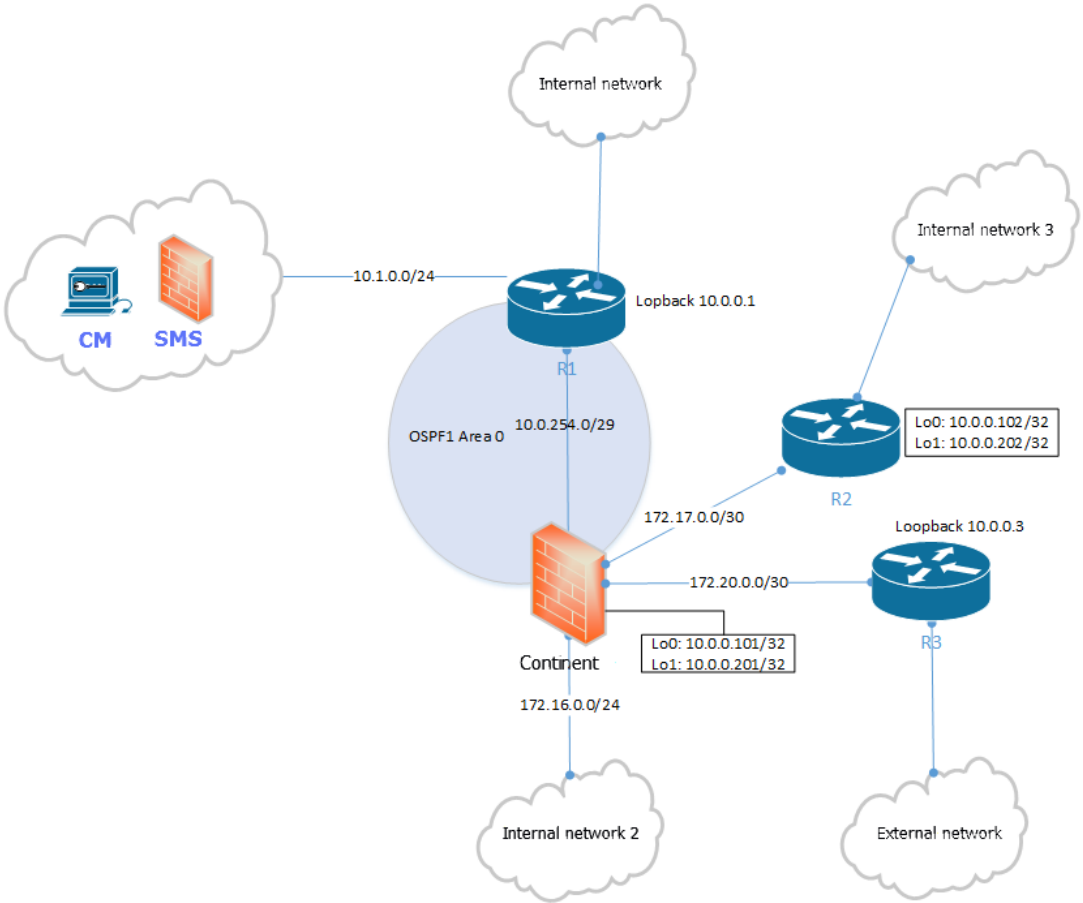
To configure dynamic routing for a Security Gateway, take the following steps:

1. Create a configuration file.
2. Enable dynamic routing on the Security Gateway and upload the configuration file to the Security Management Server database.
3. Save the changes and install the policy on the Security Gateway.

You can upload the configuration file to the Security Gateway using the local menu. This procedure is performed if there is no connection between the Security Gateway and the Security Management Server (see p. **40**).

Create a configuration file

You can see the use of a Security Gateway with dynamic routing in a network in the figure below.



There are the following routers in the system:

- router R1 has an internal network;
- router R2 has an internal network;
- router R3 has an access to extermal network.

The following virtual interfaces are configured on the Security Gateway and routers (R1–R3):

- Security Gateway — Lo0: 10.0.0.101/32, Lo1: 10.0.0.201/32;
- router R1 — Loopback 10.0.0.1;
- router R2 — Lo0: 10.0.0.102/32, Lo1: 10.0.0.202/32;
- router R3 — Loopback 10.0.0.3.

Below, you can find an example of a configuration file for this scheme.

```
#Example of dynamic protocols configuration. For more information, see
https://bird.network.cz/
router id 10.0.0.101;#---Specify the gateway ID in the ipv4 address format,
uncomment the string, e.g. "router id 10.0.0.101"---
#Dummy protocol that allows local routes to be passed to the bird table
protocol device {
      scan time 5;
}
#Dummy protocol that allows local routes to be passed to the bird table
protocol direct {
      ipv4 {
            import all;
      };
}
#Dummy protocol that allows local routes to be passed to the bird table
protocol static {
      ipv4 {
            import all;
      };
      check link on; #State of the hardware connection (reported by the OS) is taken
into account
      route 10.0.0.3/32 via 172.17.0.2; #Static routes for bird
      route 10.0.0.102/32 via 172.17.0.2; #Static routes for bird
}
#Mandatory filter restricting duplicating static and local routes from bird to
kernel
filter export_kernel {
      if source ~ [RTS_STATIC, RTS_DEVICE] then reject;
      accept;
}
protocol kernel{
      metric 0; #Parameter that allows you to specify the corresponding metric for
the routing protocols and pass routes with a metric from bird to kernel
      ipv4 {
            import none; #Restrict passing routes from kernel to master
            export filter export_kernel; #Pass routes from master to kernel except
local and static
      };
      scan time 115;
}
# Example of a function for filtering routes
#net_reserv function returns the list of networks described below
function net_reserv() {
      return net ~ [ 169.254.0.0/16+, 127.0.0.0/8+, 224.0.0.0/4+, 240.0.0.0/4+,
0.0.0.0/32-, 0.0.0.0/0{25,32}, 0.0.0.0/0{0,7} ];
}
#net_local function returns the list of networks described below
function net_local() {
      return net ~ [ 172.16.0.0/12+, 10.0.0.0/8+, 192.168.0.0/16+];
}
#import_all function for filter aggregation
function import_all() {
```

```
      if net_reserv() || net_local() then return false; #Filter restricting imports
of networks listed in the functions above
      # if bgp_path.first != 49432 then return false; #Filter restricting imports of
routes for which first as path differs from 49432
      # if bgp_path.len > 100 then return false; #Filter restricting imports of
routes if as path length exceeds 100
      # if bgp_next_hop != from then return false; #Filter restricting imports of
routes for which next hop differs from neighbor
      if dest = RTD_UNREACHABLE then return false; #Filter restricting imports of
unreachable routes
      return true;
}
#Filter using import_all function during route import
filter bgp_in {
      if ! import_all() then reject;
      krt_metric = 40; #Set a metric for 40 accepted routes
      accept;
}
#OSPF configuration section
protocol ospf ospf1{
      router id 10.0.254.1; #Specify a separate router ID if necessary
      ipv4 {
            export filter { if ( source ~ [RTS_DEVICE, RTS_BGP] ) then { accept; }
reject;}; #With redistribution of local routes and BGP
            import filter { krt_metric = 110; accept;}; #Mandatory filter that sets
the 110 metric for routes received from OSPF
      };
#backbone area
      area 0{ #Specify the area identifier, e.g. "area 0"
            networks{
            10.0.254.0/29; #Specify the subnet in the A.B.C.D/E format, e.g.
"10.0.254.0/29"
};
#Specify the networks that are not transit betweeen routers
      stubnet 172.16.0.0/24;
      stubnet 172.17.0.0/30;
      stubnet 172.20.0.0/30;
      interface "te-2-0" {#Set all interfaces that belong to the area defined in the
section, e.g. "interface "te-2-0""
      #hello 1;dead 5;retransmit 5; #Set the required timers
      authentication none; #Passwords are not sent in BFD packages. Default value
      check link on; #State of the hardware connection (reported by the OS) is taken
into account
      # cost <num>; #Specify the output cost (metric) of the interface. Default
value: 10
      };
};
}
#IBGP configuration sections
protocol bgp ibgp1{ #Specify the name of the protocol in the NAME field, e.g. ibgp1
      router id 10.0.0.101; #Specify a separate router ID if necessary
      ipv4 {
            next hop self; #Declare this router as next hop (must be used in the
neighborhood through Loopback).
            export filter { if ( source ~ [RTS_DEVICE, RTS_OSPF, RTS_OSPF_IA, RTS_
OSPF_EXT1, RTS_OSPF_EXT2] && net!=10.0.0.101/32 ) then { accept; } reject;}; #With
redistribution of local and OSPF routes
            import filter { krt_metric = 20; accept;}; #Mandatory filter that sets
the 20 metric for routes received from IBPG
```

```
            };
      local 10.0.0.101 as 65001; #Specify the gateway standalone system, e.g. "local
as 65001"
      neighbor 10.0.0.102 as 65001; #Specify the neighbor IP address and AS ibgp,
e.g. "neighbor 10.0.1.2 as 65001"
      multihop 5; #Maximum number of hops for a neighbor that is not connected
directly

}
#EBPG configuration sections
protocol bgp ebgp1{ #Specify the name of the protocol in the NAME field, e.g. ebgp1.
      router id 10.0.0.201; #Specify a separate router ID if necessary
      ipv4 {
            next hop self;#Declare this router as next hop (must be used in the
neighborhood through Loopback)
            export none; #No route redistribution
            import filter bgp_in; #Filter routes received from the neighbor
according to the previously described "bgp_in" filter
            };
      local 10.0.0.201 as 65001; #Specify gateway standalone system, e.g. "local as
65004"
      neighbor 10.0.0.3 as 65004; #Specify neighbor IP address and IBPG value, e.g.
"neighbor 10.0.1.2 as 65004"
      multihop 5; #Parameter defines the maximum number of hops for a neighbor that
is not connected directly

}
```

Create a configuration file according to the figure and example above.

For an example of a configuration file for a Security Gateway operating in virtual routing mode, see p. **42**.

Enable dynamic routing on the Security Gateway and upload the configuration file to the Security Management Server database

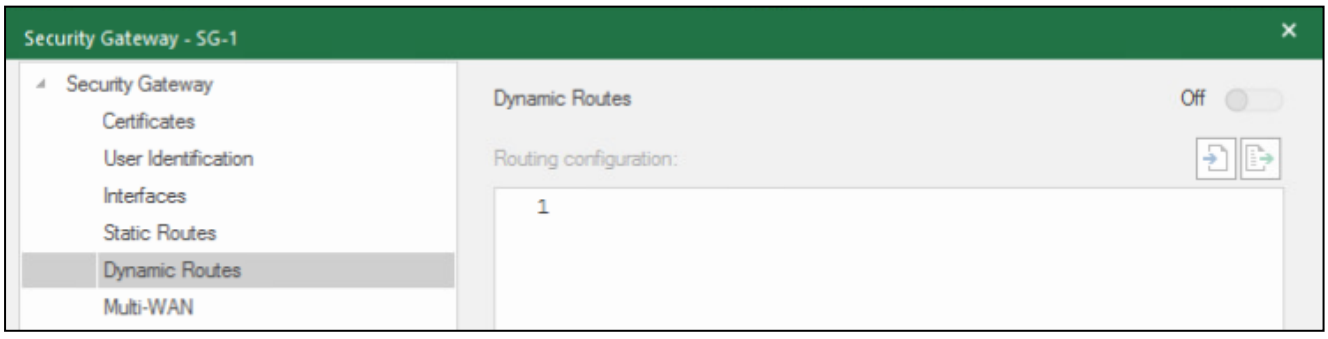
To enable dynamic routing:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway, click **Properties** and go to **Dynamic Routes** on the left.

   The respective window appears.

2. Turn on the **Dynamic Routes** toggle at the top and click **Import routing configuration**.

   File Explorer appears.



3. Specify the path to the configuration file and click **Open**.

   The configuration file will be imported to the Security Management Server database and its contents appear in the dynamic routing settings window.

Routing configuration:

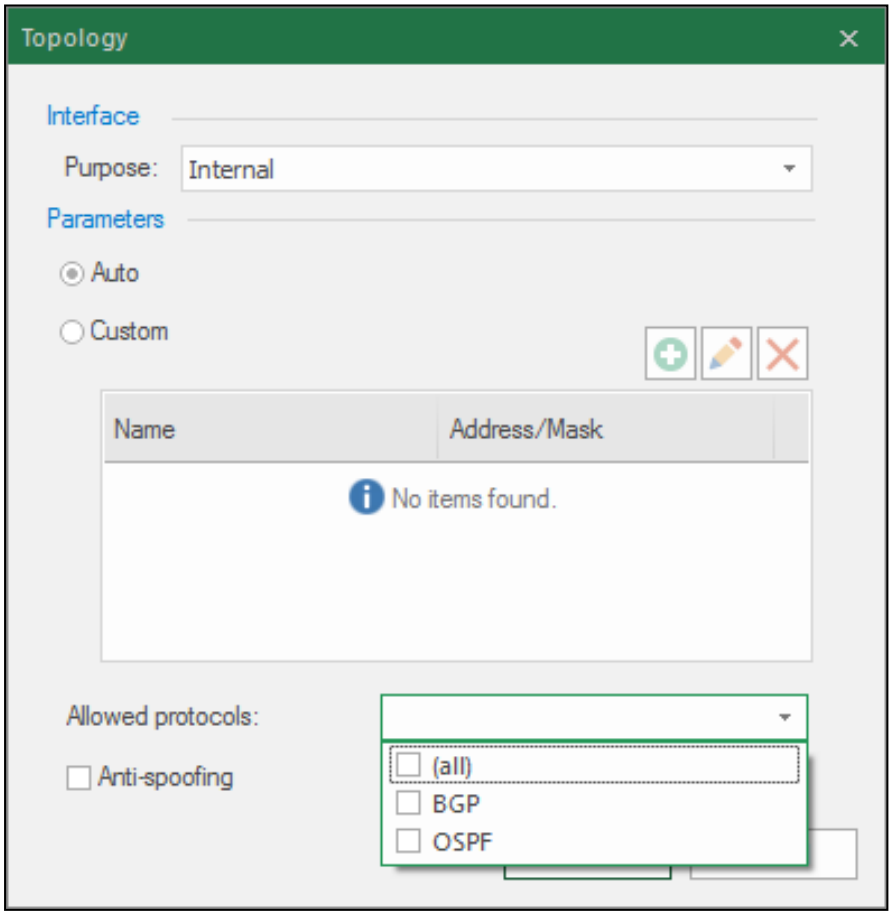
```
router id 10.0.1.4; #node ID in dynamic routing protocols
protocol direct{
    ipv4{import all;}; #transfer of local routes into dynamic protocols
}
protocol static{
    ipv4{import all;}; #transfer of static routes into dynamic protocols
filter export_kernel{
    if source ~ [RTS_STATIC, RTS_DEVICE] then reject;
    if source ~ [RTS_OSPF, RTS_OSPF_IA, RTS_OSPF_EXT1, RTS_OSPF_EXT2] then{
        krt_metric = 110;
        accept "received with ospf:", net," via ", gw;
    }
    reject;
}
protocol kernel {
    metric 0;   # to allow pepr-route metric
    ipv4 {
        import none;
        export filter export_kernel;    # Actually insert routes into the kernel routing table
    };
    scan time 5;
}

protocol ospf{
    ipv4 {
        export all;
        import all;
    };
    area 0{
        networks{
            10.0.1.0/24;
        };
        interface "te-0-0" { #list all interfaces for the OSPF protocol
```

4. Edit the contents of the file if necessary.

   If you need to export a configuration file, click and save the file.

5. On the left, go to **Interfaces**, select the interface on which you want to enable dynamic routing and double-click the **Topology** parameter.

   The respective dialog box appears (for more information on topology settings, see p. 9).



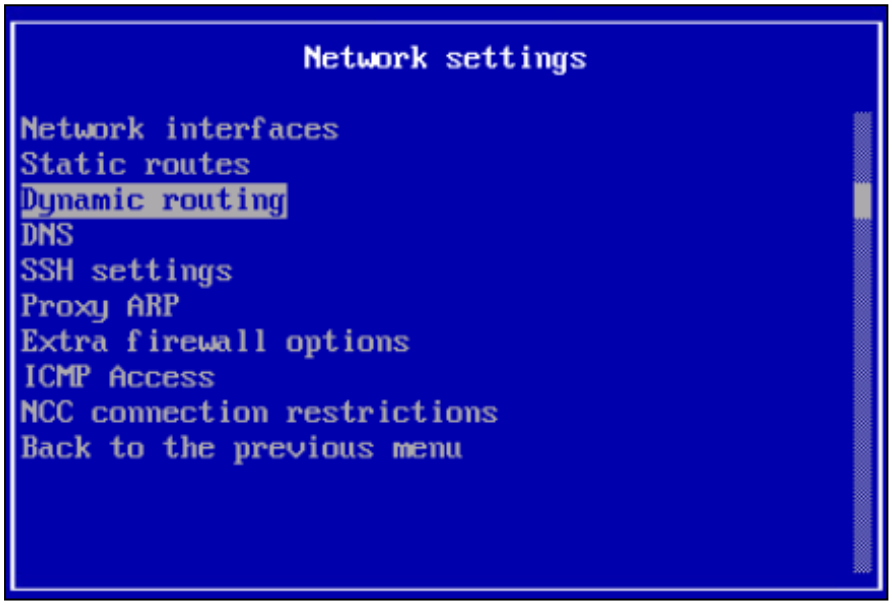
6. In the **Allowed protocols** drop-down list, select the required dynamic routing protocols (**BGP**, **OSPF** or **all**).

> **Attention!**
> A protocol must match the one specified in the configuration file.

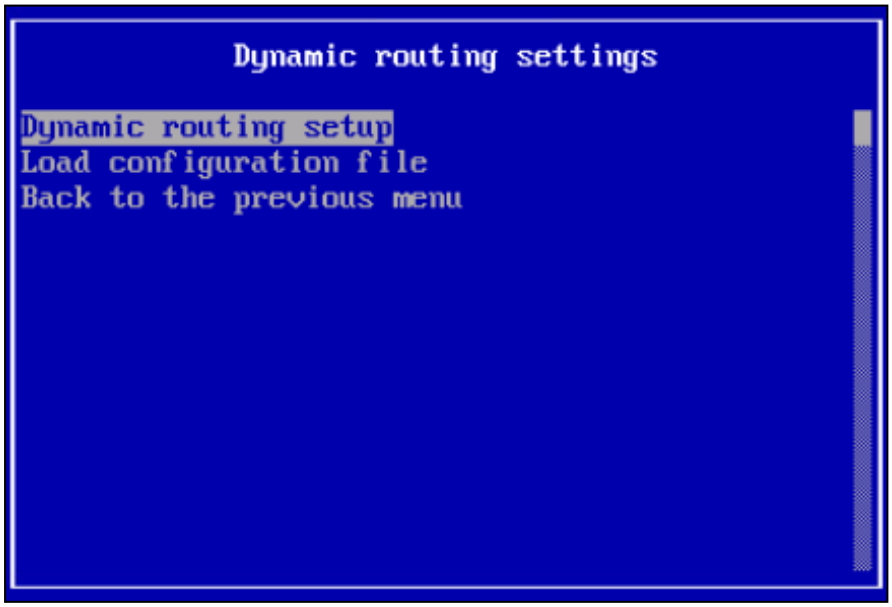
7. Click **OK**.
   The **Topology** dialog box is closed.
8. Click **OK**.
   The Security Gateway properties are closed.
9. Save the changes and install the policy on the Security Gateway with the reconfigured parameters.

Upload a configuration file using the local menu

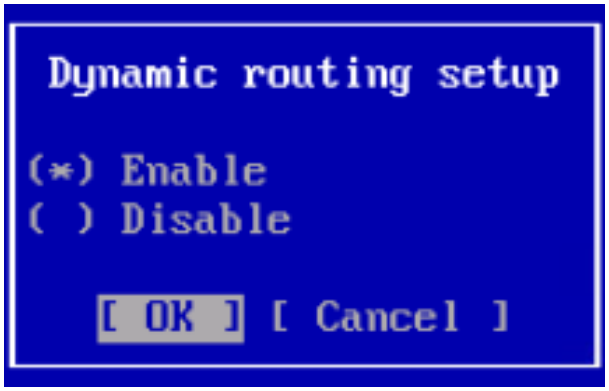
1. Prepare a USB flash drive with the configuration file.
2. In the local menu, select **Settings** | **Network** and press **<Enter>**.
   The **Network settings** window appears.



3. Select **Dynamic routing** and press **<Enter>**.
   The **Dynamic routing settings** window appears.

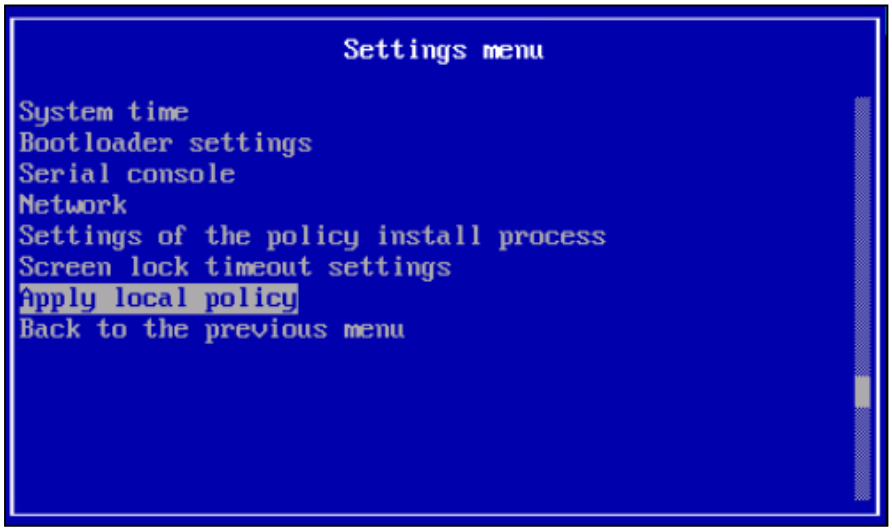


4. Select **Dynamic routing setup** and press **<Enter>**.
   The respective window appears.



5. Select **Enable** and click **OK**.
   You will be returned to the **Dynamic routing settings** window.
6. Select **Load configuration file** and press **<Enter>**.
   A message asking you to insert the USB flash drive appears.

7. Insert the USB flash drive with the configuration file and press **<Enter>**.
   A window with a list of found files appears.
8. Select the required configuration file and press **<Enter>**.
   The uploading of the configuration file to the Security Gateway starts.
   Wait for the uploading to complete.
9. Return to the settings menu and select **Apply local policy**.



   The local policies are applied.
10. Wait for the successful completion of the operation and press **<Enter>**.
    You are returned to the settings menu.
11. After restoring connection to the Security Management Server, in the Configuration Manager, go to **Structure**.
    In the list of Security Gateways, the configuration version of the Security Gateway to which the configuration file was uploaded will be displayed as **Local**.
    Select the Security Gateway and, in the context menu, select **Confirm local changes**.
    The configuration version will be changed.

Virtual routing and forwarding

Continent supports the VRF (Virtual Routing and Forwarding) mechanism. This mechanism is based on the creation and usage of VRF zones and kernel tables.

VRF zones are interfaces of a specific Security Gateway. Isolated VRF zones are created in a Security Gateway which allows processing traffic without errors even with the overlapping IP addresses.

A specific network interface can be assigned only to one VRF zone, a VRF zone can be assigned to several network interfaces. The maximum number of VRF zones supported by a Security Gateway is **255**.

Attention!
You can create and configure VRF zones only on Security gateways in UTM mode.

All packets received by an interface set by a VRF zone are handled via a respective VRF zone routing table.

Routes are transmitted between VRF zones, and the dynamic routing is possible via the Pipe protocol of BIRD. IPv4 routes are transmitted if there are no overlapping IP addresses.

VRF zones are used in Firewall and NAT filtering rules.

By default, each Security Gateway has a VRF zone with ID 0. Continent software operates in this zone, including local services that listen to incoming traffic (for example, SSH) and generate outgoing traffic (for example, NTP).

You can select the VRF zone's ID if this ID has not been taken by another VRF zone already. The ID range is from 1 to 255. The VRF zone name is generated automatically by joining a VRF zone's ID and the VRF prefix (for example, VRF-001). You cannot change a VRF zone's ID and name once it is created and a policy is applied.

The VRF-all zone is created automatically when at least one VRF zone is created. The VRF-all zone includes VRF-0 zone and all created VRF zones.

You can configure static and dynamic routing, filtering and NAT rules for all VRF zones except for the VRF-0 zone.

You can view all VRF zones in the Monitoring tool (see [**5**]).

Configure VRF zones

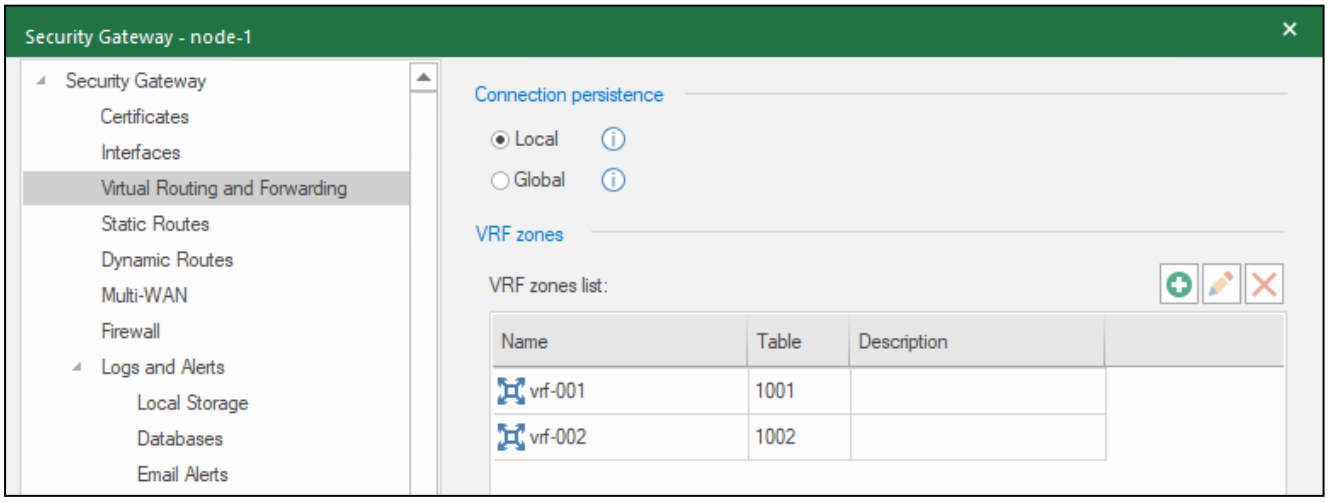
A VRF zone has the following parameters:

- name;
- description;
- list of the security gateway's interfaces;
- list of static routes used in it.

You can create and configure VRF zones in the Configuration Manager.

To work with VRF zones:

1. In the **Structure** section of the Configuration Manager, select the Security Gateway.
   In the Security Gateway context menu, select **Properties**. The respective dialog box appears.
2. In the Security Gateway properties dialog box, select **Virtual Routing and Forwarding**.
   The list of created VRF zones appears on the right.



   The list is empty if you have not created any VRF zones.

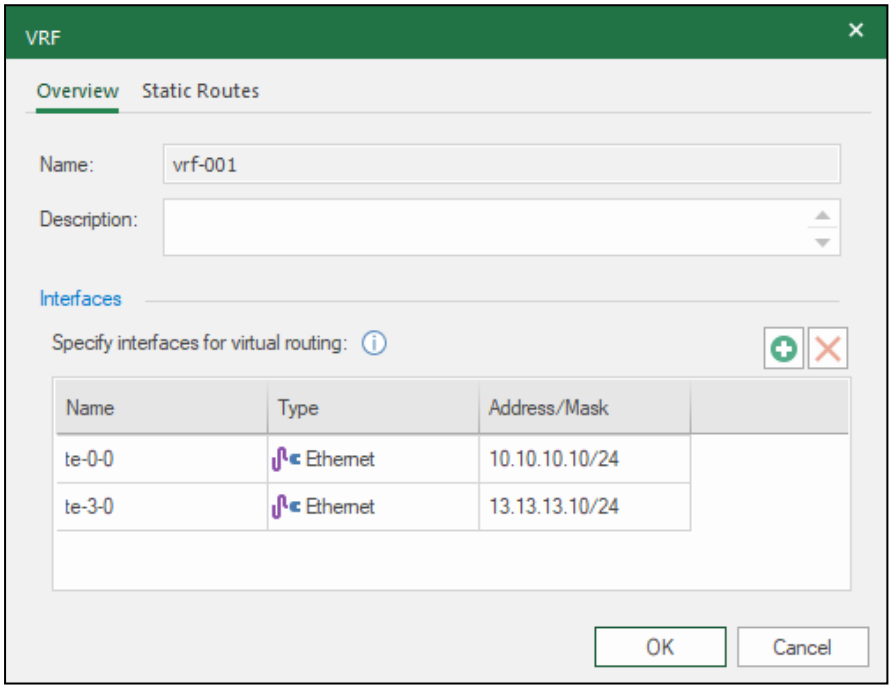
The list of VRF zones contains columns for its name, table and description.

Attention!
A VRF zone with ID 0 is not displayed in the list.

3. Specify the required connection management mode in the **Connection persistence** group of parameters:
   - **Local** – a unique session to track connections is used for each VRF zone;
   - **Global** – one session to track connections is used for all VRF zones.

To create a new VRF zone:

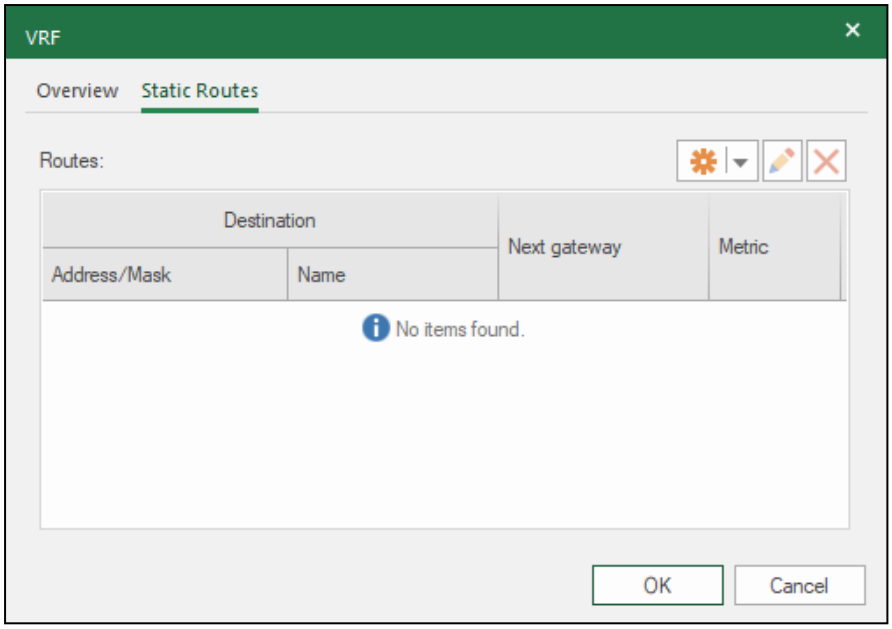
1. In the **VRF zones** section, click .
   The **Overview** tab of the **VRF** dialog box appears.



   The **ID** field is filled in automatically. If you have not created a VRF zone before, the value of the **ID** field is 1. When you create a new VRF zone, the value of this field is increased by one. If necessary, you can change the ID manually. Once you create a VRF zone, you cannot change its ID and the **ID** field is replaced with the **Name** field. It is filled in automatically in accordance with the specified ID.
2. Specify the description of a VRF zone. You can change the description later.
3. Click in the **Interfaces** section to specify the interfaces of the Security Gateway for the VRF zone.
   The list of the Security Gateway's interfaces which are included in the VRF-0 zone appears. These interfaces are not used in other components that are not supported in the VRF zones different from the VRF-0.
4. Select the interface and click **OK**.
   The selected interface appears in the table on the **Overview** tab.
5. If necessary, add other interfaces.

Attention!
Specific rules are applied when you operate with the network interfaces. For more information, see p. 45.

   To delete an interface from the list, select it and click . If an interface is deleted from the VRF zone, it is moved to the VRF-0 zone. The VRF-0 zone is not displayed in the list.
6. Go to the **Static Routes** tab.



Specify the routes for the zone. For instructions on how to create a static route list, see p. 32.

7. To save the changes, click **OK**.

   The **VRF** dialog box closes and the created VRF zone is added to the list.

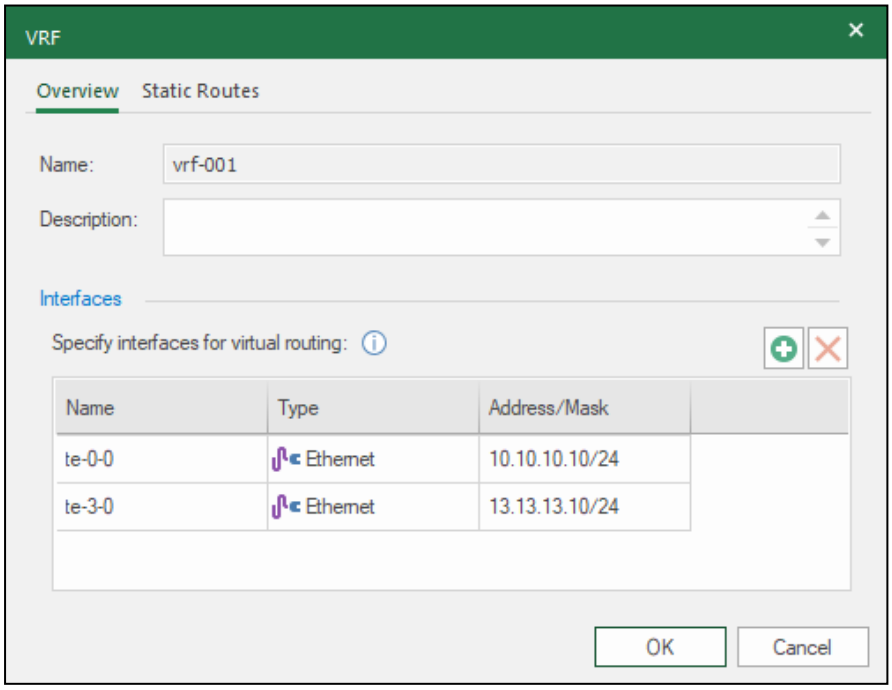
   When the VRF zone list is generated, you can edit and delete the selected VRF zone. To edit or delete a VRF zone, select it and click or .

8. When you configure the list of VRF zones, save the changes on the Security Management Server and install the policy on the Security Gateway.

To view or configure the VRF zone parameters:

1. Select the required VRF zone and click .

   The **Overview** tab of the **VRF** dialog box appears. The tab contains the VRF zone name, description and a list of its Security Gateway interfaces.



See the procedure above to configure the VRF zone. You cannot change the name of the created VRF zone.

2. Go to the **Static Routes** tab.

   The list of the static routes for the zone appears.

3. Configure the list of routes if necessary.
4. To save the changes, click **OK**.
   The **VRF** dialog box closes. The list of VRF zones is displayed.
5. Save the changes on the Security Management Server and install the policy on the Security Gateway.

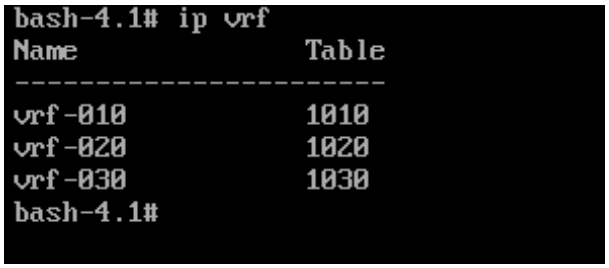
View information about VRF zones using the local management tools

You can view the following information about VRF zones using the local management tools:

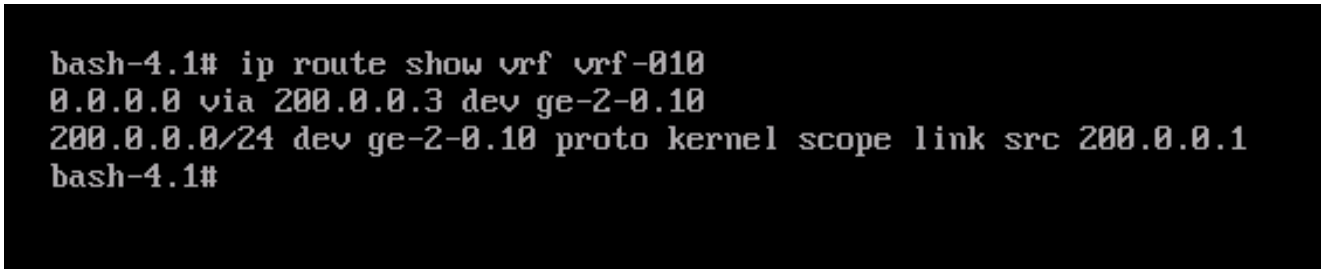
- list of the created VRF zones;
- static route table of a specific VRF zone;
- traffic flow in a specific zone.

To view information about a VRF zone:

1. In the main menu of the required Security Gateway, select **Tools** | **Diagnostics** | **Command line**.
   The **Continent Shell** appears.
2. To view the list of the Security Gateway's VRF zones, run the following command:
   ```
   ip vrf
   ```
   The list of all VRF zones of the Security Gateway with their tables appears.

3. To view the list of the static routes in the zone, run the following command:
   ```
   ip route show vrf <VRF zone name>
   ```
   The list of the static routes in the specified VRF zone appears. In this example, the vrf-010 zone has only one static route.

4. To view the packet flow in the VRZ zone, run the following command:
   ```
   tcpdump -i <VRF zone name>
   ```
   The data about the specified VRF zone traffic appears.

Configure network interfaces of VRF zone

The following rules are applied when you work with the network interfaces:

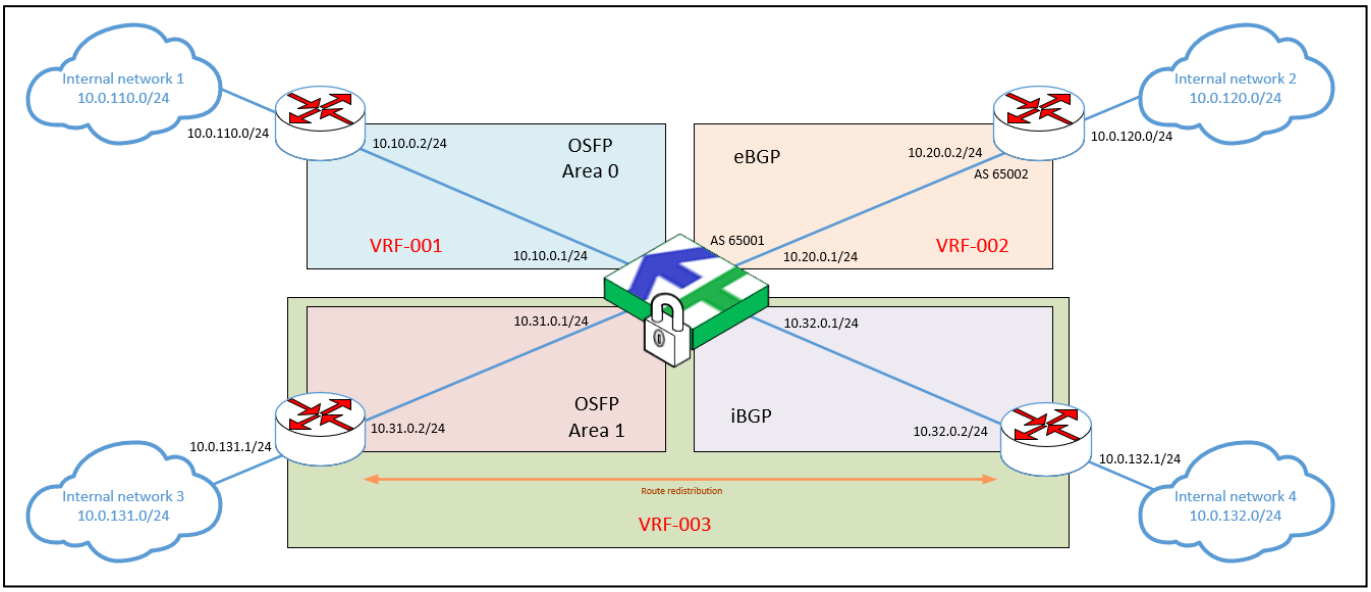
- If you create a subordinate network interface, it is included in the same VRF zone as the primary interface.
- If you change the VRF zone of the primary interface and if its subordinate interfaces are in the same VRF zone, subordinate interfaces are moved to a new VRF zone of the primary interface.
- VLAN interfaces can be included in other VRF zones if their primary interface is in the VRF-0 zone.
- If you create a bond interface, select its contents from the VRF-0 zone.
- If you change a VRF zone for a bond interface, interfaces included in the bond interface are moved to the specified VRF zone.

- If you add an interface to a bond interface, the added interface is transferred to the selected bond interface.
- If you exclude an interface from a VRF zone, it is transferred to the VRF-0 zone.
- You cannot add loopback and bridge interfaces and interfaces with the Switch port topology to a VRF zone (see p. **43**).
- If you change the topology of the interface included in the VRF zone different from the VRF-0, you cannot select the Switch port topology.

Example of a configuration file for dynamic routing

This section contains an example of a configuration file for the dynamic routing on the Security Gateway with the usage of a VRF zone.

Routers are used to connect internal networks to a Security Gateway (see the figure below).



Three VRF zones (VRF-001 – VRF-003) are created on the Security Gateway.

Internal network 1 uses the table of the VRF-001 zone. The OSPF protocol is used to exchange information between Security Gateway and router about the routes.

Internal network 2 uses the table of the VRF-002 zone. The eBGP protocol is used to exchange information between Security Gateway and router about the routes.

An internal network 3 and 4 can communicate via a Security Gateway using the VRF-003 table. The exchange between the Security Gateway and the router of Internal network 3 is based on the OSPF protocol. The exchange between the Security Gateway and the router of Internal network 4 is based on the iBGP protocol.

Routes from table VRF-002 can be transferred to table VRF-003 through the Pipe protocol.

You can see the configuration file for this scheme below.

```
Configuration file
router id 10.35.1.1; #Router ID for a node
#Protocol to scan an interface state
protocol device {
      scan time 2;
}

#Protocol to monitor interfaces
protocol direct {
}

#Additional routing tables to use in VRF != 0
ipv4 table vrf_1;
ipv4 table vrf_2;
ipv4 table vrf_3;

#Protocol to get the direct routes of the VRF zones
```

```
protocol direct D_VRF_1 {
      vrf "vrf-001";
      ipv4 { table vrf_1; };
}

protocol direct D_VRF_2 {
      vrf "vrf-002";
      ipv4 { table vrf_2; };
}

protocol direct D_VRF_3 {
      vrf "vrf-003";
      ipv4 { table vrf_3; };
}

#Protocol to synchronize the bird routes with the OS core routes
protocol kernel vrf_001{
      vrf "vrf-001"; #VRF number
      kernel table 1001; #Table number in the system (1000 + VRF number)
      learn 1;
      scan time 20;
      metric 0;
      ipv4 {
            table vrf_1; #Table name created before
            import all;
            export all;
      };
}

protocol kernel vrf_002{
      vrf "vrf-002"; #VRF number
      kernel table 1002; #Table number in the system (1000 + VRF number)
      learn 1;
      scan time 20;
      metric 0;
      ipv4 {
            table vrf_2; #Table name created before
            import all;
            export all;
      };
}

protocol kernel vrf_003{
      vrf "vrf-003"; #VRF number
      kernel table 1003; #Table number in the system (1000 + VRF number)
      learn 1;
      scan time 20;
      metric 0;
      ipv4 {
            table vrf_3; #Table name created before
            import all;
            export all;
      };
}

#Filter specifying a metric and
filter vrf_import
prefix set allowed_prefs; #Declare a list variable
{
```

```
      if net ~ [10.35.1.0/24, 10.10.0.0/24, 10.20.0.0/24, 10.31.0.0/24,
10.32.0.0/24] then reject "my local address advert rejected"; #Restrict receiving of
local network adverts
      if net.ip = gw then reject;
      allowed_prefs=[10.0.0.0/8{16,32}]; #List of routes allowed to be imported
      if net ~ allowed_prefs then {
            krt_metric = 10;
            accept; }
      else {
            reject; }
}

#OSPF in VRF-1 zone
protocol ospf peer1 {
      router id 10.10.0.1;
      vrf "vrf-001";ipv4 {
            table vrf_1;
            import filter vrf_import;
            export none; #Without routes redistribution
      };
      area 0 {
            networks {10.10.0.0/24;};
            interface "te-1-0" {
            hello 10;
            dead 40;
            retransmit 5;
            authentication none;
            };
      };
}

#BGP in VRF-2 zone
protocol bgp ebgp1{
      router id 10.20.0.1;
      vrf "vrf-002";
      ipv4 {
            table vrf_2;
            import filter vrf_import;
            export filter { if ( net = [10.20.0.0/24] ) then { reject; } accept;};
      };
      local as 65000; #Number of a local AS
      neighbor 10.20.0.2 as 65001; #Neighbor IP address and AS number
      source address 10.20.0.1; #IP address to build a connection (is not necessary
if you configure ebgp)
      multihop 3; #Number of hops to build a connection. Default value: 1
}

#OSPF in VRF-3 zone
protocol ospf ospf2 {
      router id 10.31.0.1;
      vrf "vrf-003";
      ipv4 {
            table vrf_3;
            import filter vrf_import;
            export filter { if ( net = [10.31.0.0/24] ) then { reject; } accept;}
#With the redistribution of VRF zone routes except for routes to the neighbor
      };
      area 0 {
            networks {10.31.0.0/24;};
            interface "te-3-0" {
```

```
            hello 10;
            dead 40;
            retransmit 5;
            authentication none;
            };
      };
}

#Protocol to transfer routes between VRF zones
protocol pipe {
      table vrf_2;
      peer table vrf_3;
      export filter {
            if net ~ [ 10.0.0.0/8+] then {
            if preference>10 then preference = preference-10;
            accept;
            }
            reject;
            };

            import filter {
            if net ~ [ 10.0.0.0/8+] then {
            if preference>10 then preference = preference-10;
            accept;
            }
            reject;
      };
}
#BGP protocol in VRF-3 zone
protocol bgp ibgp1{
      router id 10.32.0.1;
      vrf "vrf-003";
      ipv4 {
            table vrf_3;
            next hop self;
            import filter vrf_import;
            export filter { if ( net = [10.32.0.0/24] ) then { reject; } accept;};
#With the redistribution of the VRF zone routes except for the routes to the
neighbor
      };
      local as 65001; #Number of the local AS
      neighbor 10.20.0.2 as 65001; #Neighbor IP address and AS number
      source address 10.32.0.1; #IP address to build a connection (is not necessary
if you configure ebgp)
      multihop 3; #Number of hops to build a connection. Default value: 1
}
```

Example of using VRF zones

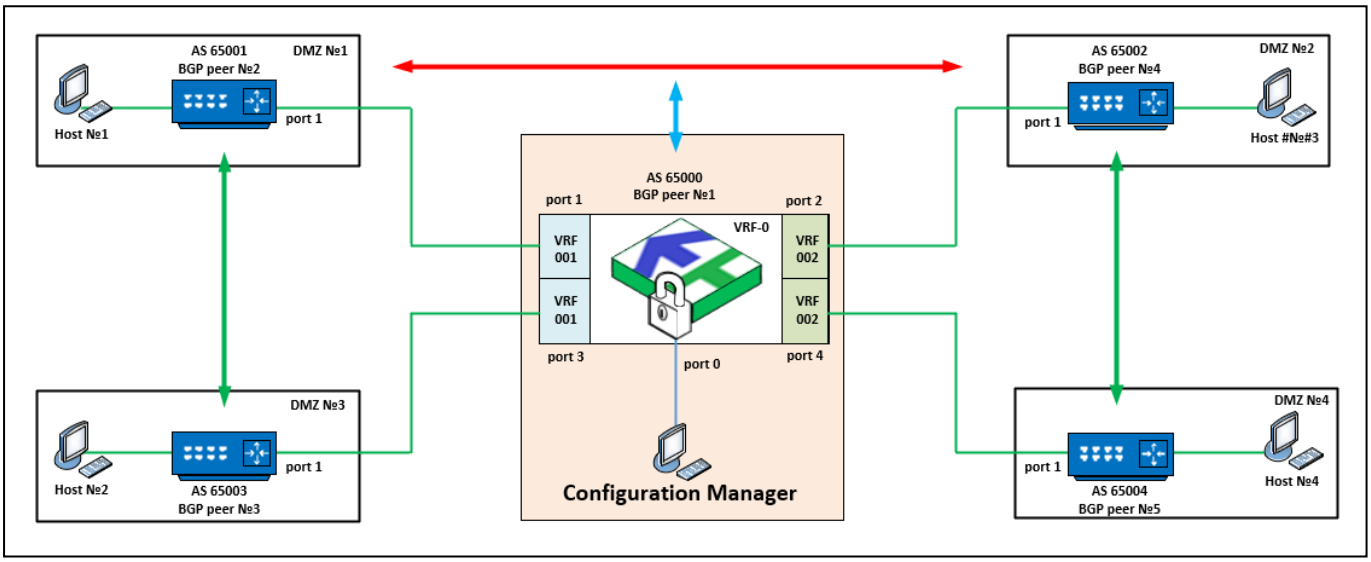
This section contains examples of using VRF zones in dynamic routing, rules for filtering and translation of the network addresses.

In the following examples, 4 routers are connected to a Security Gateway which is connected to one host. The VRF-001 and VRF-002 zones are configured on the Security Gateway. The Security Gateway is managed by an administrator via the Configuration Manager.

Isolated VRF zones

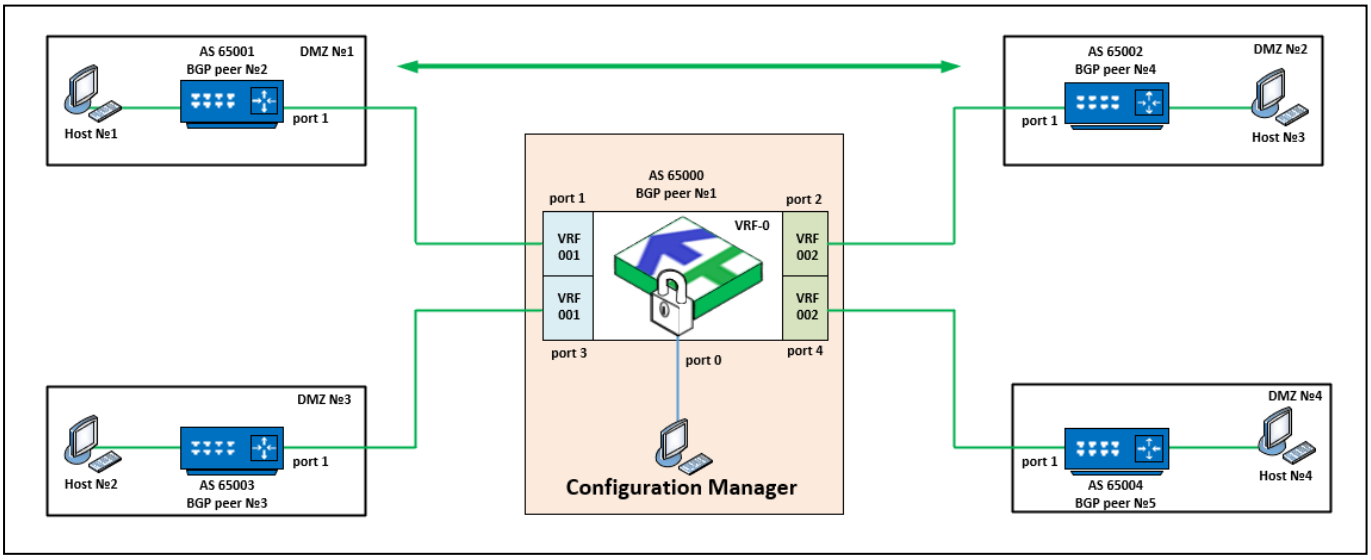
The dynamic routing is configured via the BIRD service and the BGP protocol. When the configuration file is uploaded and the policy is applied to the scheme (see the figure below), there are two groups of hosts (the left one and the right on in the scheme) whose ports belong to different VRF zones (VRF-001 and VRF-002).

Hosts of the left and right zones can be connected with each other only in their VRF zone. Hosts from one VRF zone do not have a connection with hosts from other VRF zones.



Transfer routes between VRF zones

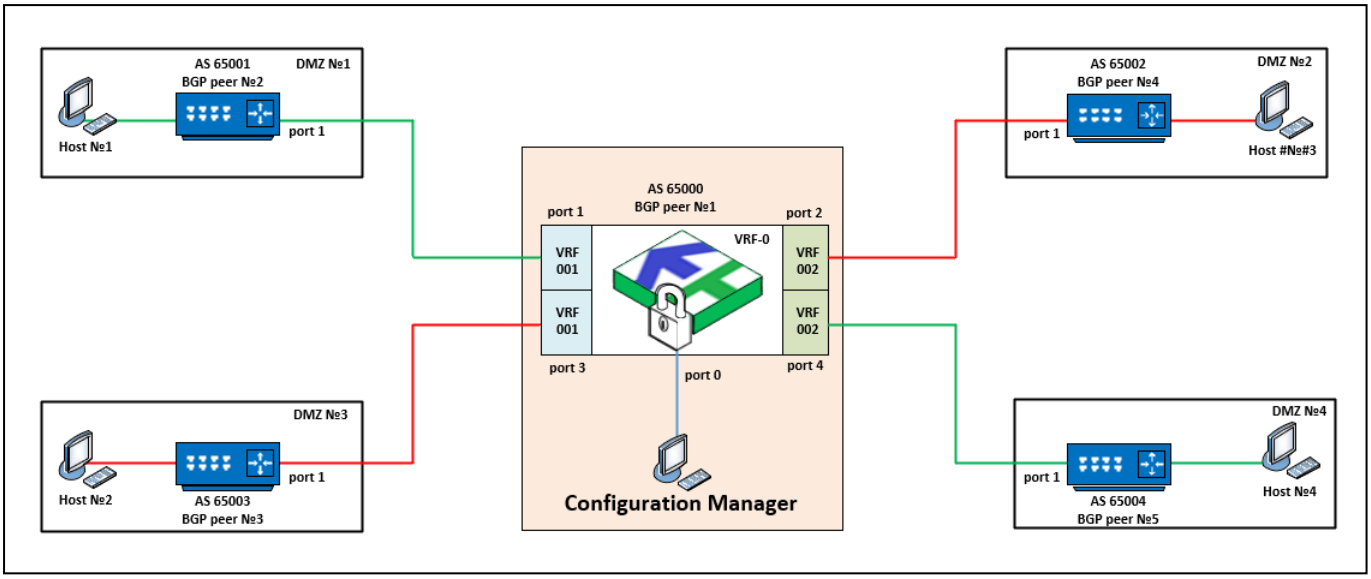
In this case, if you use the Pipe protocol in the configuration file for transferring routes between VRF zones, you can connect hosts of different VRF zones: hosts of the VRF-001 zone can establish connection with hosts of the VRF-002 zone. Hosts in the VRF-002 zone can be connected to hosts in the VRF-001 zone.



Firewall rules

In the Firewall filtering rules, you can specify the VRF zone for which the rules are applied. By doing that, you can establish routing between specific hosts in the zone.

For example, you need routing between Host №1 and Host №4. To do that, create two allowing rules and specify the required VRF zones in them. In the rule with the Host №1 as a source, specify VRF-001 in the **VRF** field. In the rule with the Host №4 as a source, specify VRF-002 (see the figure below).



When the policy is applied, only one routing channel through both VRF zones operates based on the configuration files settings.

Static routing with address space intersection

This section contains examples of using VRF zones in static routing.

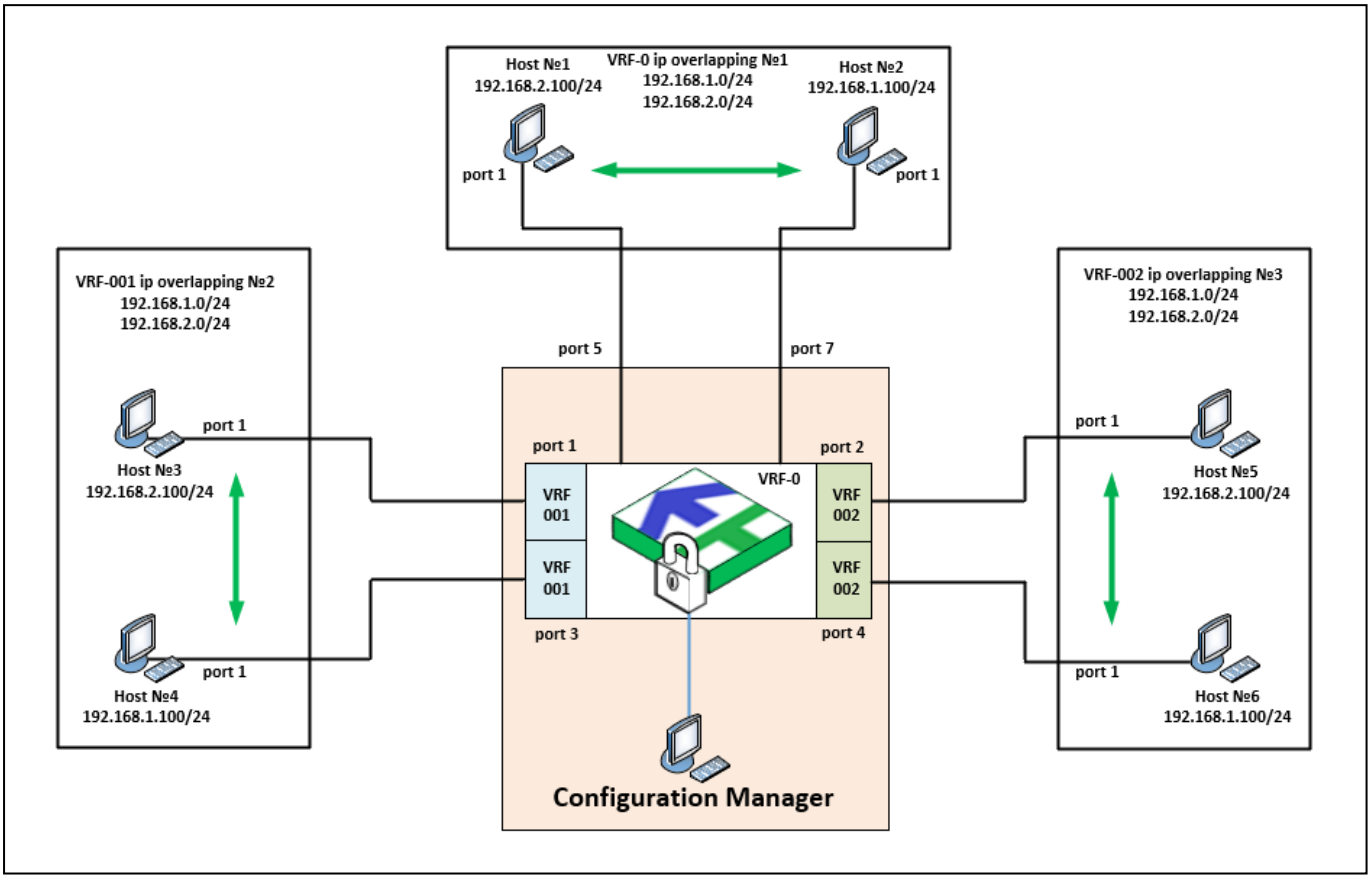
In the following examples, three host groups with the same IP addresses are connected to a Security Gateway. The VRF-001 and VRF-002 zones are configured on the Security Gateway. The interfaces of Host №1 and Host №2 belong to one group.

The Security Gateway is managed by an administrator via the Configuration Manager.

Routing between hosts in one VRF zone

Without the use of separate routing tables, traffic cannot pass between hosts within its virtual routing table because route overlap occurs.

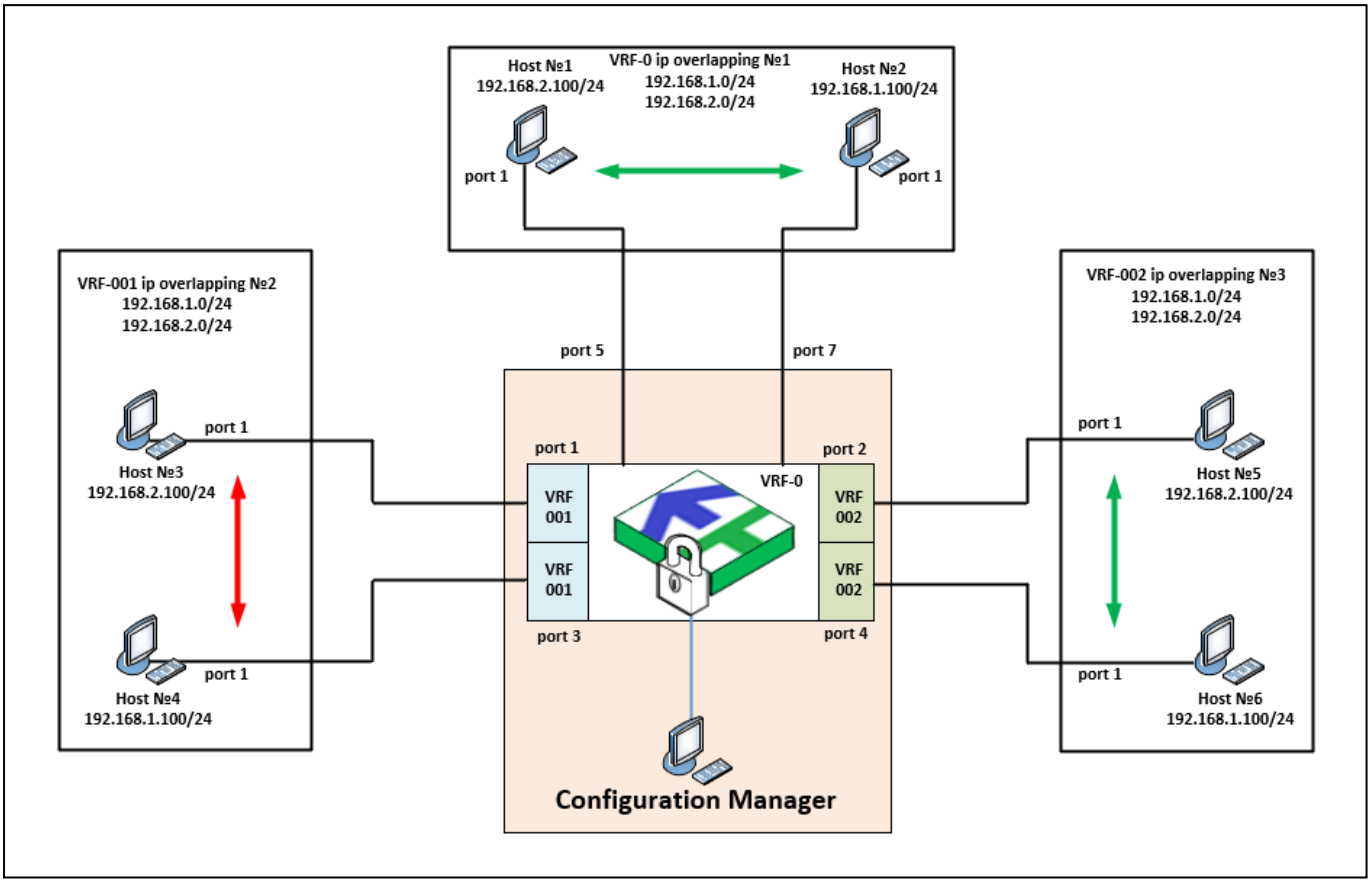
To allow traffic to pass within the zone, you must create a filtering rule on the Security Gateway for all-to-all access. Specify the VRF-all zone including VRF-001, VRF-002 and VRF-0 zones as a VRF zone in the filtering rule.



When the policy is applied, traffic can pass between hosts in each zone (VRF-001, VRF-002 and VRF-0).

Traffic restriction in a VRF zone

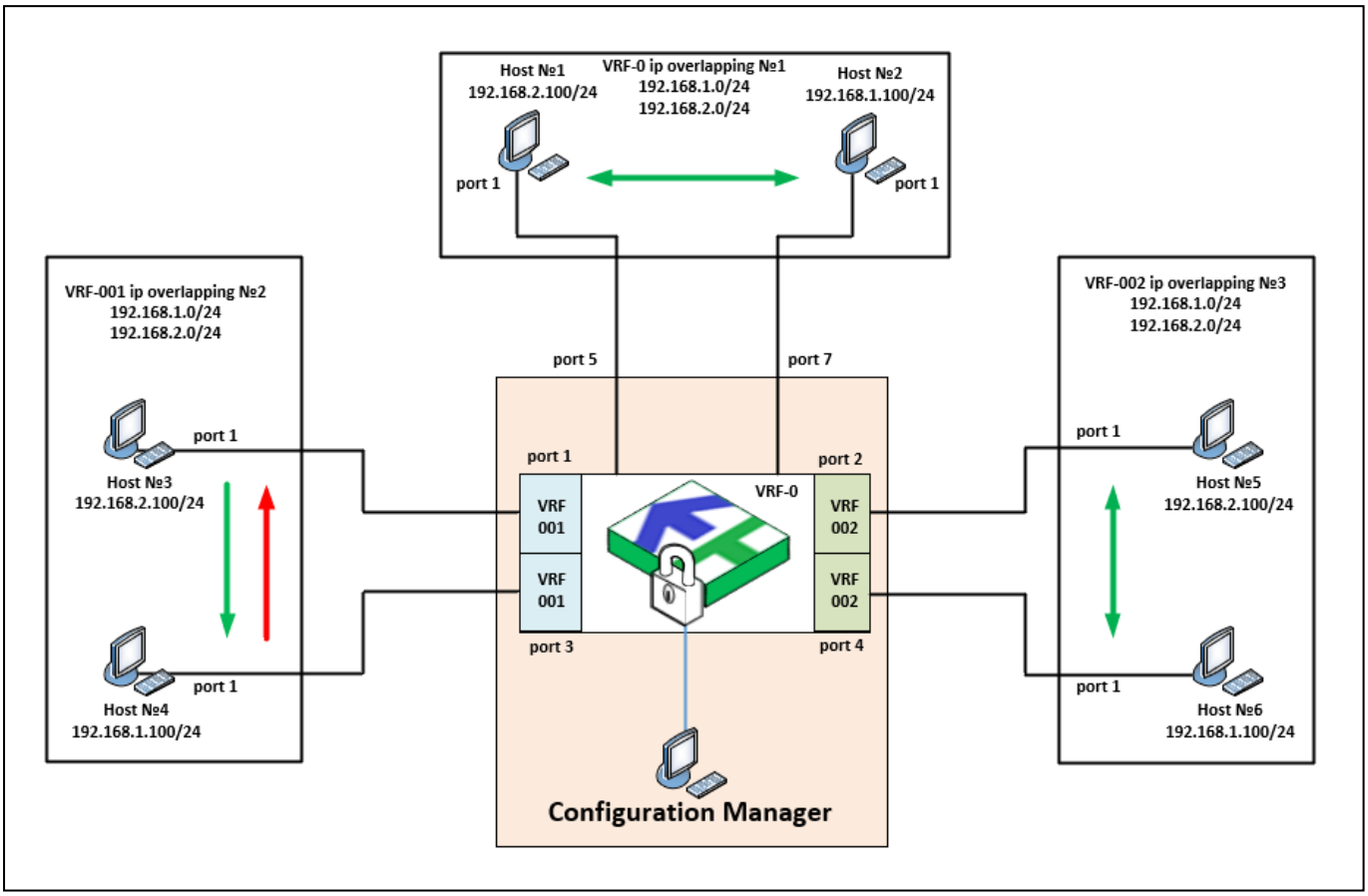
To deny traffic between hosts within any VRF zone (for example, VRF-001 as in the figure below), you must use filtering rules. Specify a Security Gateway and specify VRF-001 in the **VRF** column without specifying it in the filtering rule. Select **Drop** in the **Action** column.



When the policy is applied in the VRF-0 and VRF-002 zones, hosts can connect to each other, and Host №3 and Host №4 in the VRF-001 zone cannot establish connections with each other (routing is absent).

Routing restrictions in a VRF zone

An example below shows the routing restrictions in a VRF zone. For example, Host №3 can connect to Host №4 in the VRF-001 zone and Host №4 cannot connect to Host №3. The restriction is performed via two filtering rules for the VRF-001 zone. In the first rule, traffic from the source (Host №3) to the destination (Host №4) is allowed. In the second rule, traffic from the destination (Host №4) to the source (Host №3) is restricted.

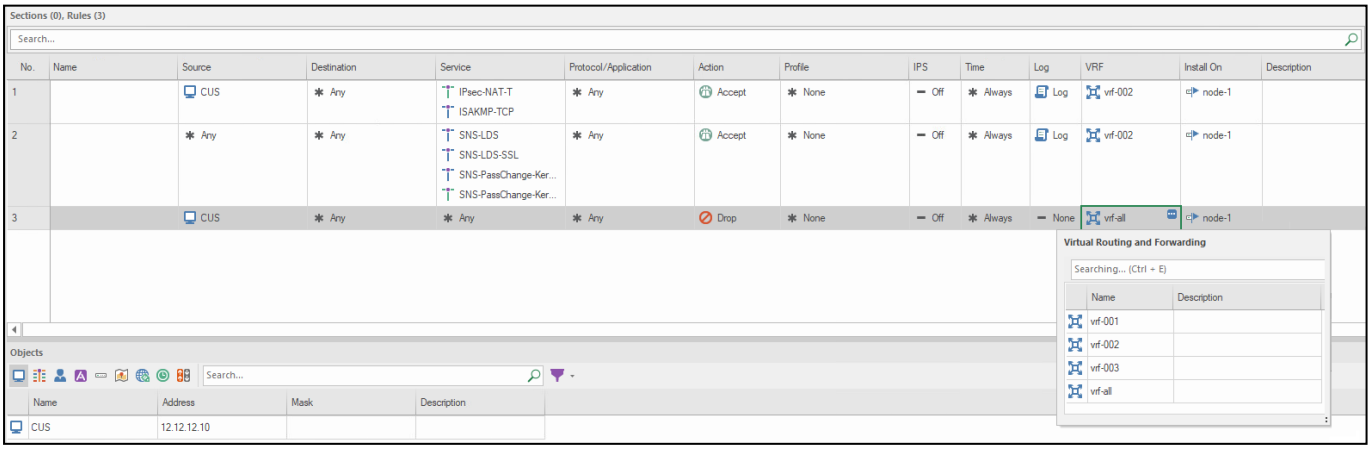


Configure Firewall

Firewall filtering rules can be applied to the VRF zones of Security Gateways.

To apply rules to a VRF zone:

1. In the Configuration Manager, go to **Access control** | **Firewall**.
   The list of rules appears in the display area.



2. Select or create the required rule.
3. In the **Install On** column, select a Security Gateway to apply the rule.

4. In the **VRF** column, click . The **Virtual Routing and Forwarding** dialog box appears. Select the VRF zone to apply the rule.

   Attention!
   If you select a VRF zone for a cluster, only cluster VRF zones are displayed in the **Virtual Routing and Forwarding** table.

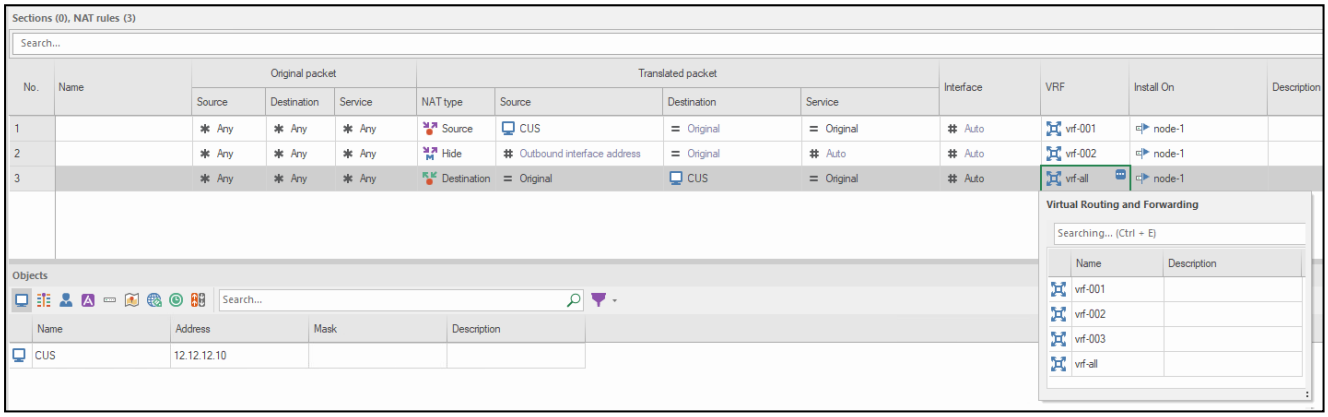
5. Apply the policy.

Configure NAT rules

NAT rules can be applied to the VRF zones of Security Gateways.

To apply rules to a VRF zone:

1. In the Configuration Manager, go to **Access control** | **NAT**.
   The list of rules appears in the display area.



2. Select or create the required rule.
3. In the **Install On** column, select a Security Gateway to apply the rule.
4. In the **VRF** column, click . The **Virtual Routing and Forwarding** dialog box appears. Select the VRF zone to apply the rule.

   Attention!
   If you select a VRF zone for a cluster, only cluster VRF zones are displayed in the **Virtual Routing and Forwarding** table.

5. Apply the policy.

VRF zones in a cluster

For more information on how to create and configure a cluster, see [**6**].

If a Security Gateway with virtual routing is included in a cluster, the VRF zone number is displayed in the list of interfaces.

Configure network interfaces of a VRF zone in a cluster

Note the following rules and restrictions while working with network interfaces in a cluster:

- internal or external physical interfaces of a cluster can be added only to the VRF-0 zone;
- a subordinate network interface is automatically added to the VRF-0 zone;
- only cluster network interfaces can be edited in the Cluster properties dialog box;
- all network interfaces except for cluster ones can be edited in the Security Gateway properties dialog box.

Physical interfaces

You can do the following to configure physical interfaces in the Security Gateway properties and Cluster properties dialog boxes:

- change a topology;
- change protocols (OSPF, BGP, BFD);
- change a role or enable/disable the monitoring;
- include interfaces with the **Cluster**, **1st sync**, **2nd sync** and **Private** roles in the VRF-0 zone;

- specify two IP addresses for interfaces with the **1st sync** role;
- specify three IP addresses for interfaces with the **2nd sync** and **Cluster** roles.

VLAN interfaces

You can do the following to configure VLAN interfaces in the Security Gateway properties and Cluster properties dialog boxes:

- change a topology;
- create an interface (in a Security Gateway or a cluster);
- change protocols (OSPF, BGP, BFD);
- change a role or enable/disable the monitoring;
- include a VLAN interface to all VRF zones (including the VRF-0 zones with the **Cluster** role);
- include interfaces with the **1st sync** role to the VRF-0 zone;
- specify one IP address for an interface with the **1st sync** role if it is in the VRF-0 zone;
- specify up to three IP addresses for interfaces with the **Cluster** role if they are in the VRF-0 zone;
- specify one IP address for an interface with the **Cluster** role if it is in the VRF-0 zone.

Bond interfaces

You can do the following to configure bond interfaces in the Cluster properties dialog box:

- change a topology;
- create an interface (in a Security Gateway or a cluster);
- change protocols (OSPF, BGP, BFD);
- change a role or enable/disable the monitoring;
- include interfaces with the **Cluster** or **1st sync** roles in the VRF-0 zone;
- specify one IP address for an interface with the **Cluster** role;
- specify up to three IP addresses if they are in the VRF-0 zone.

Loopback interfaces

You can do the following to configure loopback interfaces of a Security Gateway included in a cluster in the Security Gateway properties dialog box:

- change a topology (it is required to specify the protocols);
- create an interface on a Security Gateway;
- change protocols (OSPF, BGP, BFD);
- change a role or enable/disable the monitoring;
- include an interface with the **None** topology in the VRF-0 zone;
- specify one IP address for an interface with the **None** topology.

Bridge interfaces

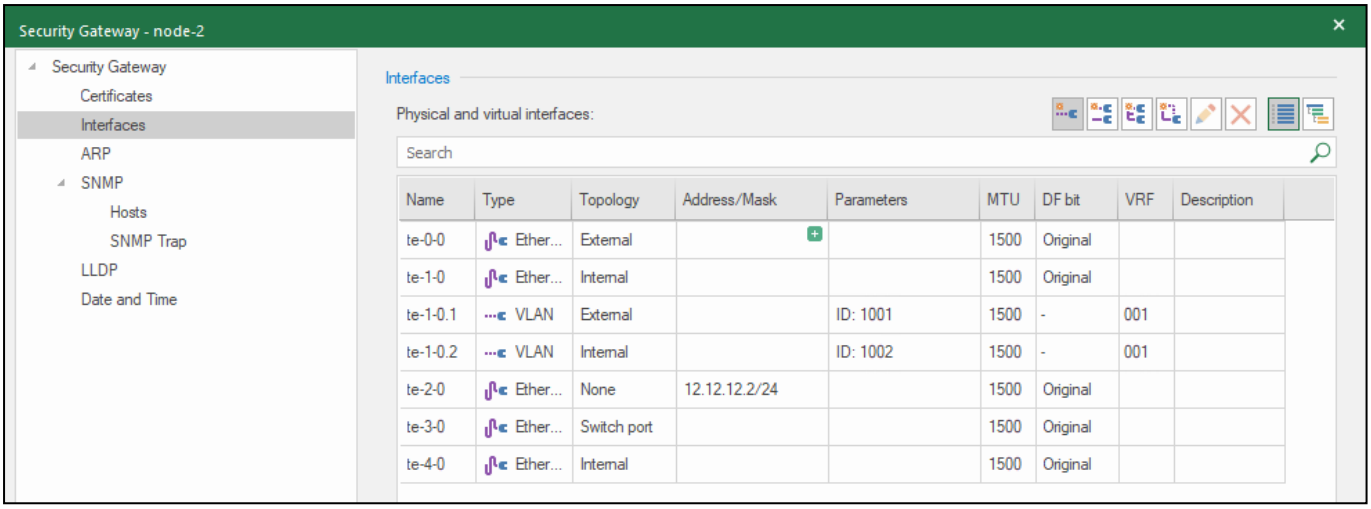
You can do the following to configure the bridge interfaces of a Security Gateway included in a cluster in the Security Gateway properties dialog box:

- change a topology;
- create an interface on a Security Gateway;
- change protocols (OSPF, BGP, BFD);
- change a role or enable/disable the monitoring;
- include an interface with the **1st sync** role in the VRF-0 zone.

Configure Security Gateway in a cluster

Once a Security Gateway is included in a cluster, the **Virtual Routing and Forwarding**, **Static Routes** and **Dynamic Routes** groups of parameters become unavailable for editing. These settings are automatically transferred to a cluster.

If a VRF zone includes the interfaces of a Security Gateway, these VRF zones are displayed in the list of interfaces.

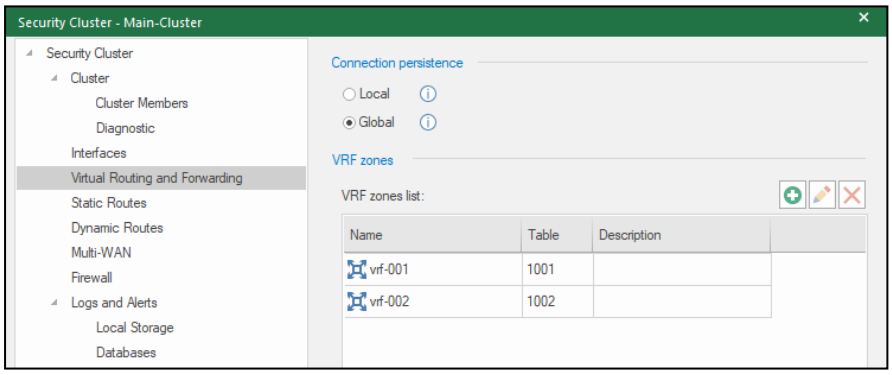


Configure VRF zone in a cluster

You can configure the VRF zones of the cluster in the Cluster properties dialog box.

To create or edit a VRF zone in a cluster:

1. Go to **Structure**, select the required cluster and click **Properties**.
2. In the **Properties** dialog box, select **Virtual Routing and Forwarding**.
   The list of VRF zones appears on the right.



3. Click to create a new VRF zone.
   The **VRF** dialog box appears.
4. Specify the required parameters.
   To edit a VRF zone, click and make the required changes.

DNS

You can configure DNS using either the Configuration Manager or the local menu.

To configure DNS using the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.
2. On the left, select **DNS**.

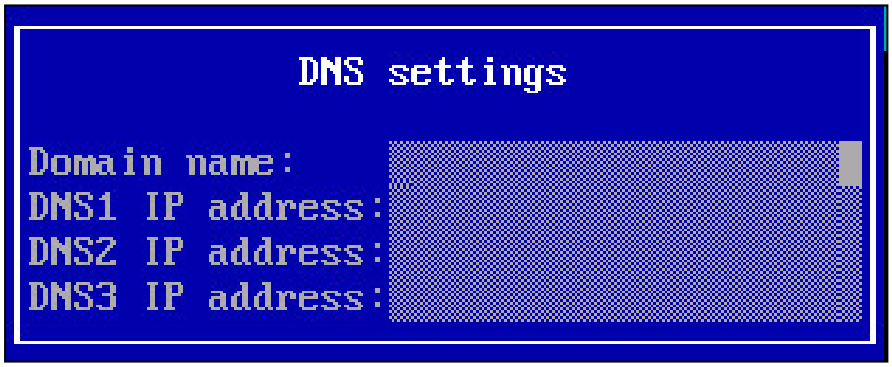
The list of DNS servers appears on the right.

Attention!
If a DNS server is available but cannot resolve a particular domain name, the Security Gateway does not attempt to obtain the IP address of that domain name through the following listed DNS servers.

3. Enter the IP address of a preferred DNS server and alternate ones if necessary, then click **OK**.
4. Save changes and install the policy on the Security Management Server.
   Wait for the installation to be completed.

To configure DNS using the local menu:

1. In the main menu, select **Settings** and press **<Enter>**.
   The respective menu appears.
2. Select **Network** and press **<Enter>**.
   The network settings of the Security Gateway appear.
3. Select **DNS** and press **<Enter>**.
   The **DNS settings** dialog box appears.



4. Enter a DNS suffix, the IP address of a preferred DNS server, the IP addresses of alternate DNS servers if they exist. Press **<Enter>**.

Note.
To move through menu sections, use the navigation keys <↑> and <↓>.

Attention!
If a DNS server is available but cannot resolve a particular domain name, the Security Gateway does not attempt to obtain the IP address of that domain name through the following listed DNS servers.

5. Go back to **Settings**, select **Apply local policy** and press **<Enter>**.

Note.
When you change the configuration locally, you can apply the local policy only once.

6. Confirm changes in the Security Management Server configuration by clicking the respective button in the Configuration Manager.

ARP

You can view, create, edit, update and delete entries in the ARP table and configure a Proxy ARP. This can be done via Configuration Manager or the Monitoring tool via the web console.

An administrator can do the following with static entries in the Configuration Manager:

- create;

- view;
- edit;
- delete.

Also, Proxy APR can be configured in the Security Gateway properties dialog box of the Configuration Manager.

An administrator can do the following with the entries in the Monitoring tool:

- view static and dynamic entries;
- update dynamic entries;
- delete dynamic entries from the ARP table.

ARP entries management and Proxy APR configuration are available when a Security Gateway is in UTM mode.

If a Security Gateway is restarted, static ARP entries and Proxy ARP entries are restored from the configuration.

Static ARP entries and Proxy APR management are not supported for clusters. It is available only for Security Gateways in a cluster.

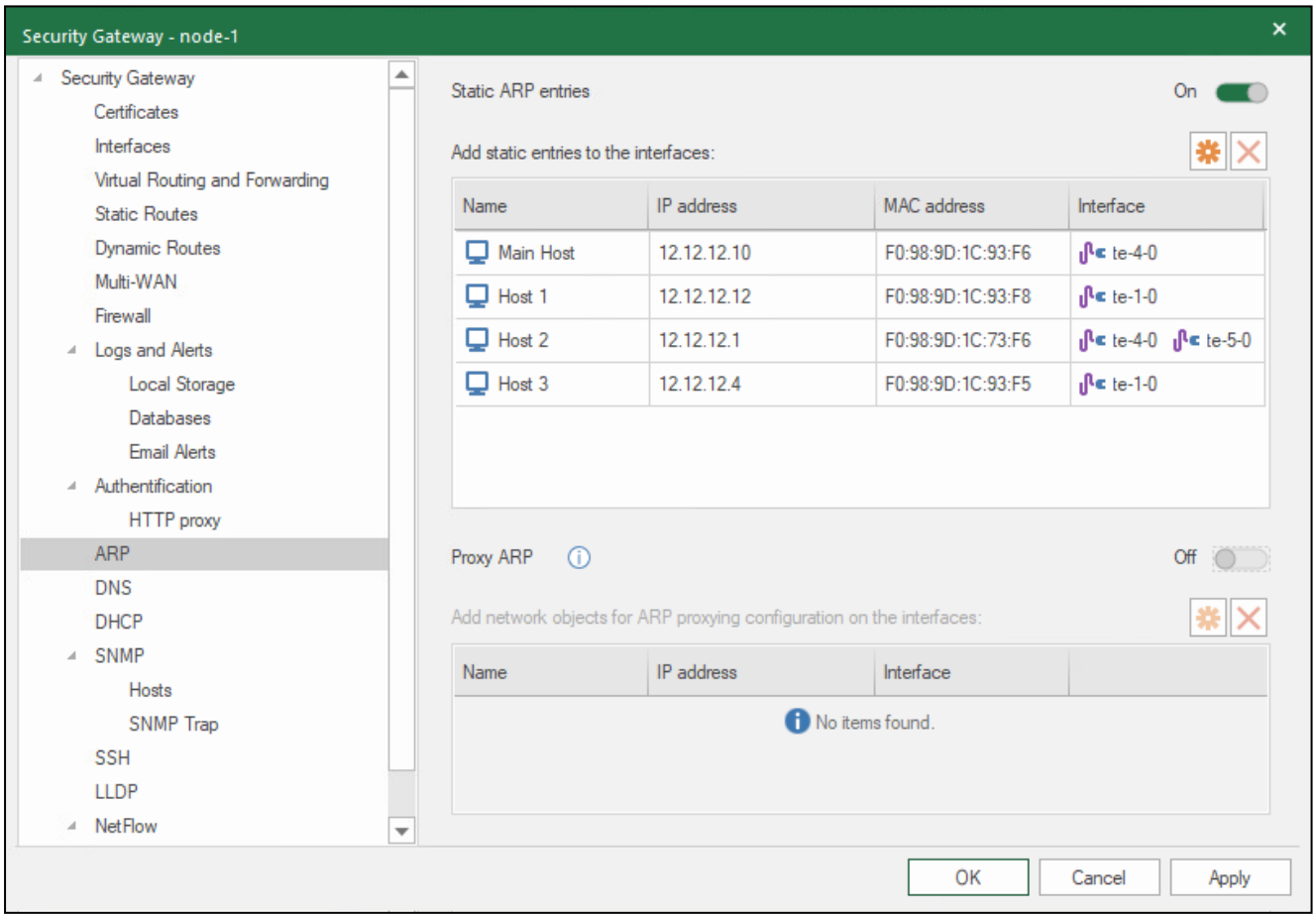
The maximum number of static ARP entries for a Security Gateway is **512**.

The maximum number of Proxy ARP entries for a Security Gateway is **128**.

By default, the ARP configuration is disabled after a Security Gateway initialization. ARP entries and Proxy ARP configuration are absent.

To configure ARP using the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.
2. On the left, select **ARP**.
   The **Static ARP entries** and **Proxy ARP** lists appear on the right.



   If you configure them for the first time, the lists are empty.
3. To view the tables and edit them, turn on the toggles in the **Static ARP entries** and **Proxy ARP** group of parameters.

Configure Proxy ARP

Configuration of NAT rules on the Security Gateways may require additional proxy configuration to respond to incoming ARP requests.

A Security Gateway can respond to ARP requests from one network segment to another segment. All the Security Gateways of the first network consider that the Security Gateway from another network is in their segment.

You can configure Proxy ARP either manually or automatically.

Automatic configuration uses IP addresses specified in the translated packet of the SNAT and DNAT rules (see below).

To configure Proxy ARP manually, use the Configuration Manager or the local menu of the required Security Gateway (see p. **63**).

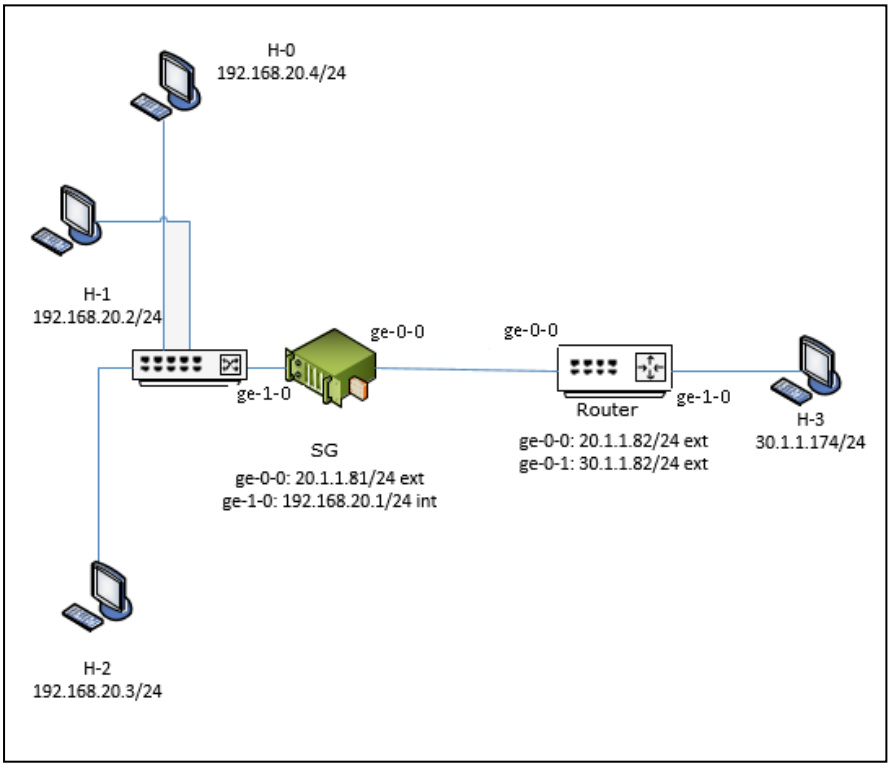
Attention!

Only one configuration mode can be active at a time. After the software installation and NAT rule configuration in the Configuration Manager, automatic configuration of Proxy ARP is enabled on the Security Gateway by default. If you change the configuration locally on the Security Gateway, manual configuration of Proxy ARP is enabled. To return to the automatic configuration, remove the local one.

Automatic configuration

If the network address of the source or destination in a translated packet of a NAT rule overlaps the address specified on an interface, a Proxy API consisting of the former network is assigned to the interface with the specified address.

The figure below illustrates examples of Proxy ARP automatic configuration.



Example 1

Create the following rule for a Security Gateway shown in the figure above:

Original packet			Translated packet		
Source	Destination	Service	NAT type	Source	Destination
192.168.20.0/24	30.1.1.0/24	Any	Source	20.1.1.71	Original

Original packet	
Source	192.168.20.0/24

Original packet	
Destination	30.1.1.0/24
Service	Any

Translated packet	
NAT type	Source
Source	20.1.1.71
Destination	Original

According to this rule, Proxy ARP for the **20.1.1.71** IP address is automatically configured on the Security Gateway **ge-0-0** interface, which means that the Security Gateway responds to arp requests from both **20.1.1.81** and **20.1.1.71** IP addresses.

Example 2

Create the following rule for a Security Gateway shown in the figure above:

Original packet			Translated packet		
Source	Destination	Service	NAT type	Source	Destination
30.1.1.0/24	20.1.1.77	Any	Destination	= Original	192.168.20.3

Original packet	
Source	30.1.1.0/24
Destination	20.1.1.77
Service	Any

Translated packet	
NAT type	Destination
Source	Original
Destination	192.168.20.3

According to this rule, Proxy ARP for the **20.1.1.77** IP address is automatically configured on the Security Gateway **ge-0-0** interface, which means the Security Gateway responds to arp requests on both **20.1.1.81** and **20.1.1.77** IP addresses.

Example 3

This example illustrates a rule according to which automatic configuration of Proxy ARP is not required. Create the following rule for a Security Gateway shown in the figure above:

Original packet			Translated packet		
Source	Destination	Service	NAT type	Source	Destination
192.168.20.0/24	30.1.1.0/24	Any	Source	40.1.1.173	= Original

Original packet	
Source	192.168.20.0/24
Destination	30.1.1.0/24
Service	Any

Translated packet	
NAT type	Source
Source	40.1.1.173

Translated packet	
Destination	Original

Proxy ARP is not required because the **40.1.1.173** IP address does not belong to the **20.1.1.0/24** network which contains **20.1.1.81** — the Security Gateway IP address, so in this case, Proxy ARP cannot be configured.

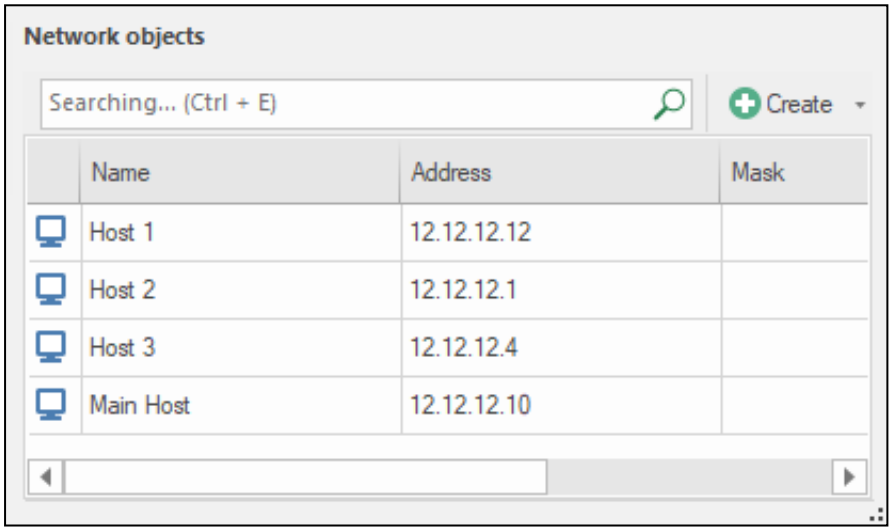
Manual ARP Proxy configuration

To create an ARP Proxy entry:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar. The respective dialog box appears. On the left, select **ARP**.
2. If the **Static ARP entries** toggle is turned off, turn it on.

   The **Add** button becomes available.
3. Click **Add**.

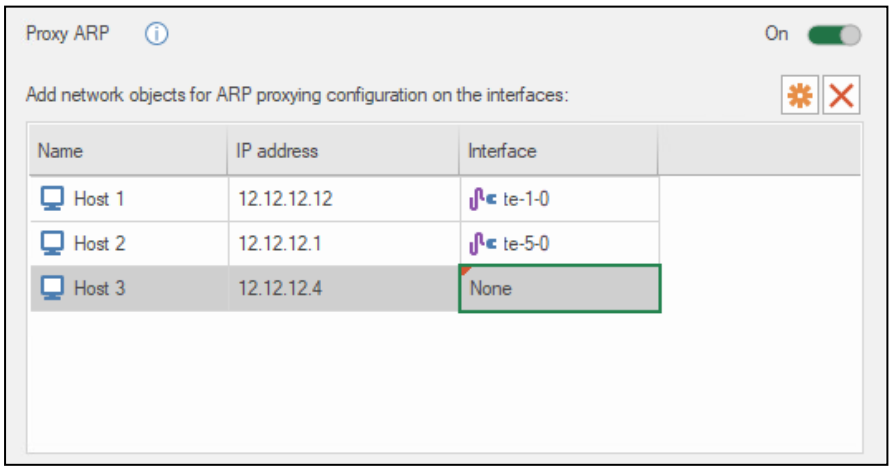
   The **Network objects** dialog box appears.



4. Select the required network object in the list.

Note.
If necessary, you can create a new network objects. To do that, click **Create** and specify the required parameters in the **Name**, **Description** and **Address** fields.

A new network object is added to the list of the ARP Proxy objects.



The name and IP address of a new entry are filled in automatically (see the figure above).

5. To specify the interface, click  and select check boxes of the required interfaces. Click **OK**.

   The selected interface(s) appears in the Interface column.

6. Click **Apply** to save changes.
7. Close the Security Gateway properties window and install the policy on the Security Gateway.
   After the policy is applied, the configuration is sent to the Security Gateway.

To change a Proxy ARP entry:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar. The respective dialog box appears. On the left, select **ARP**.
2. If the **Proxy ARP** toggle is turned off, turn it on.
3. To specify the interface, click  and select check boxes of the required interfaces. Click **OK**.
4. Double-click the **Name** and **IP address** cells, the **Host** dialog box appears.
5. Specify the required parameters and click **OK**.
6. Click **Apply** to save the changes.
7. Install the policy on the required Security Gateway.
   After the policy is applied, the configuration is sent to the Security Gateway.

To delete a Proxy ARP entry:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.
2. On the left, select **ARP**. If the **Proxy ARP** toggle is turned off, turn it on.
3. Select the entry to be deleted and click **Remove**.
   A dialog box prompting you to confirm the deletion of this entry appears.
4. Click **Yes**.
   An entry is deleted from the table.
5. Click **Apply** to save the changes.
   The Security Gateway properties window closes.
6. Install the policy on the required Security Gateway.
   After the policy is applied, the configuration is sent to the Security Gateway.

Configure Proxy ARP using the local menu

To configure Proxy ARP:

1. In the local menu, select **Settings** and press <**Enter**>.
   The respective menu appears.
2. Select **Network** and press <**Enter**>.
   The **Network** settings menu appears.
3. Select the interface that receives ARP requests for the required IP addresses and press <**Enter**>.
   The list of IP addresses for Proxy ARP appears.
4. Enter IP addresses or subnets and press <**Enter**>.
   The proxy configuration of the selected interface is changed. You are returned to the **Proxy ARP** menu.
5. Repeat steps **3** and **4** for other interfaces if necessary.
6. Select **Back to the previous** menu and press <**Enter**>. Then, select **Apply changes** and press <**Enter**>.
7. To apply the changes, select **Apply** changes.
8. Wait for the operation to be completed and confirm changes in the Security Management Server local menu or using the Configuration Manager.

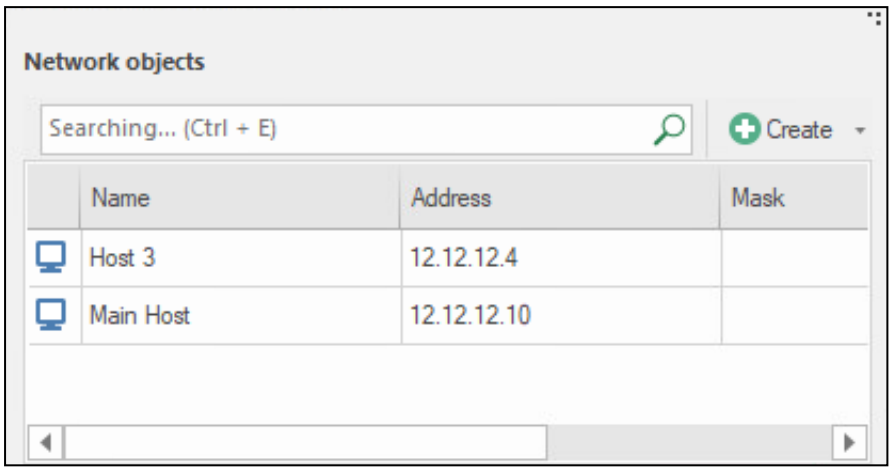
Configure APR entries

You can view, configure, change, update and delete APR entries in the APR tables using the Configuration Manager. You can view static APR entries in the local menu, too.

To create a static ARP entry:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar. The respective dialog box appears. On the left, select **ARP**.

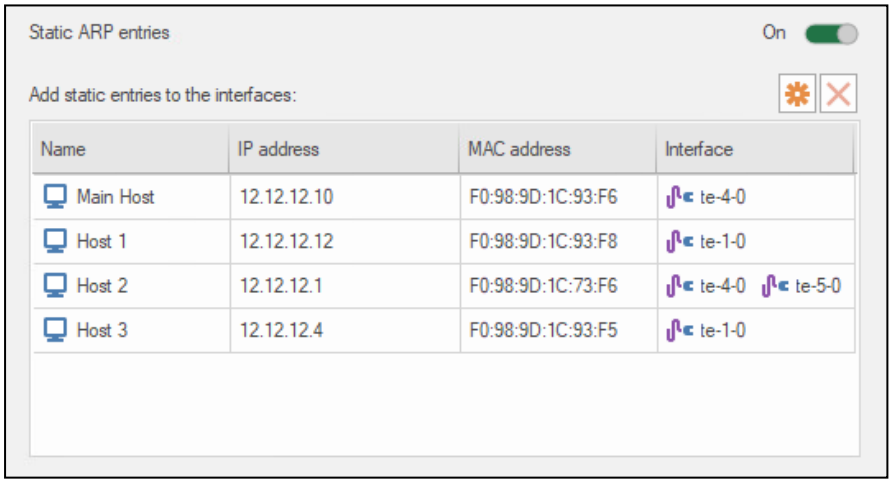
2. Turn on the **Static ARP entries** toggle.
   The **Add static ARP entry** button becomes available.
3. Click it.
   The **Network objects** dialog box appears.



4. Select the required network object in the list.

Note.
If necessary, you can create a new network objects. To do that, click **Create** and specify the required parameters in the **Name**, **Description** and **Address** fields.

A new entry is added to the list of ARP entries.



The name and IP address of a new entry are filled in automatically (see the figure above).

5. Specify the MAC address in the respective column.
6. To specify the interface, click and select check boxes of the required interfaces. Click **OK**.
   The selected interfaces appear in the **Interface** column.
7. Click **Apply** to save the changes.
8. Close the Security Gateway properties window and install the policy on the Security Gateway.
   After the policy is applied, the configuration is sent to the Security Gateway.

To change a static ARP entry:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar. The respective dialog box appears. On the left, select **ARP**. In the **Static ARP entries** table, select the required entry.
2. Change the **MAC address** cell value manually.
3. Change the interface by clicking and selecting check boxes of the required interfaces.
4. Double-click the **Name** and **IP address** cells, the **Host** dialog box appears. Specify the required parameters and click **OK**.

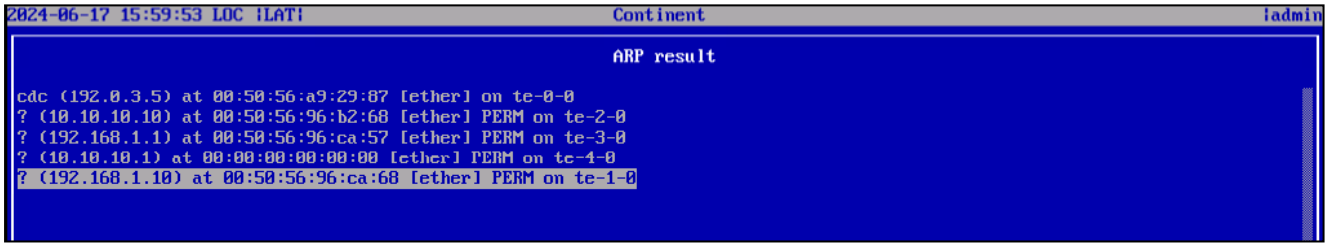
5. Click **Apply** to save the changes.
6. Close the Security Gateway properties window and install the policy on the required Security Gateway.

To delete a static ARP entry:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.
2. On the left, select **ARP**. If the **Static ARP entries** toggle is turned off, turn it on.
3. Select the entry to be deleted and click **Remove static ARP entry**.
   A dialog box prompting you to confirm the deletion of this entry appears.
4. Click **Yes**.
   An entry is deleted from the table.
5. Click **Apply** to save the changes.
   The Security Gateway properties window closes.
6. Install the policy on the required Security Gateways.
   The configuration is sent to the Security Gateway.

To view local entries in the local menu:

- In the main menu of the required Security Gateway, select **Tools** | **Diagnostics** | **Network diagnostics** | **ARP**.
  The list of ARP entries appears.



You can also view the list of ARP entries using the command line. In the main menu of the required Security Gateway, select **Tools** | **Diagnostics** | **Command line** and run the following command:

```
arp -a
```

QoS

For detailed information about QoS, see [**1**].

You can manage QoS using the Configuration Manager.

Configure QoS

The QoS configuration procedure includes the following steps:

- enable the QoS component for a Security Gateway;
- create QoS rules;
- create profiles for inbound and outbound traffic and apply QoS rules to them;
- assign traffic profiles to Security Gateway interfaces.

Enable QoS

To enable QoS:

1. In the Configuration Manager, go to **Structure**.
   The list of Security Gateways appears.
2. Select the required Security Gateway and click **Properties** on the toolbar.
3. In the **Components** group box, select the **QoS** check box and click **Apply**.
   On the left, the **QoS** menu item appears.
4. To save the profile, click **OK**.

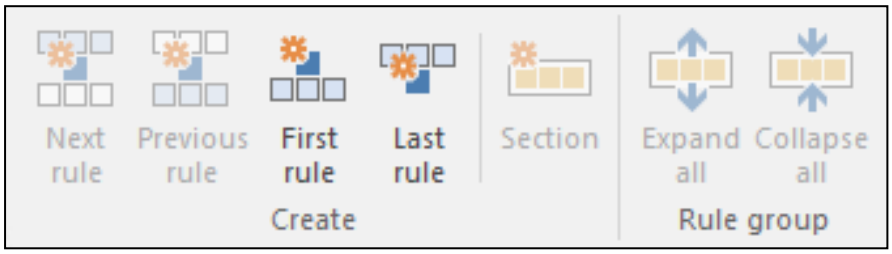
The **Security Gateway** dialog box is closed.

Attention!
The operation of the **QoS** component with services configured for DPI and Ipoque is not guaranteed.

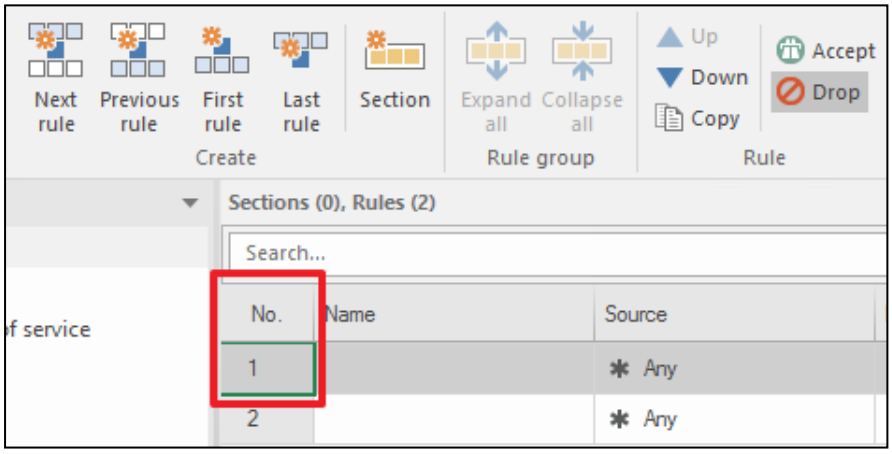
Create QoS rules

To create a QoS rule:

1. In the Configuration Manager, go to **Access control** | **QoS**.
2. On the toolbar, select the type of a rule you want to create and click the respective button.



- If the list of rules is empty, you can click only **First rule** and **Last rule**.
- To create the next or previous rule, select a rule created earlier and click the respective button on the toolbar.



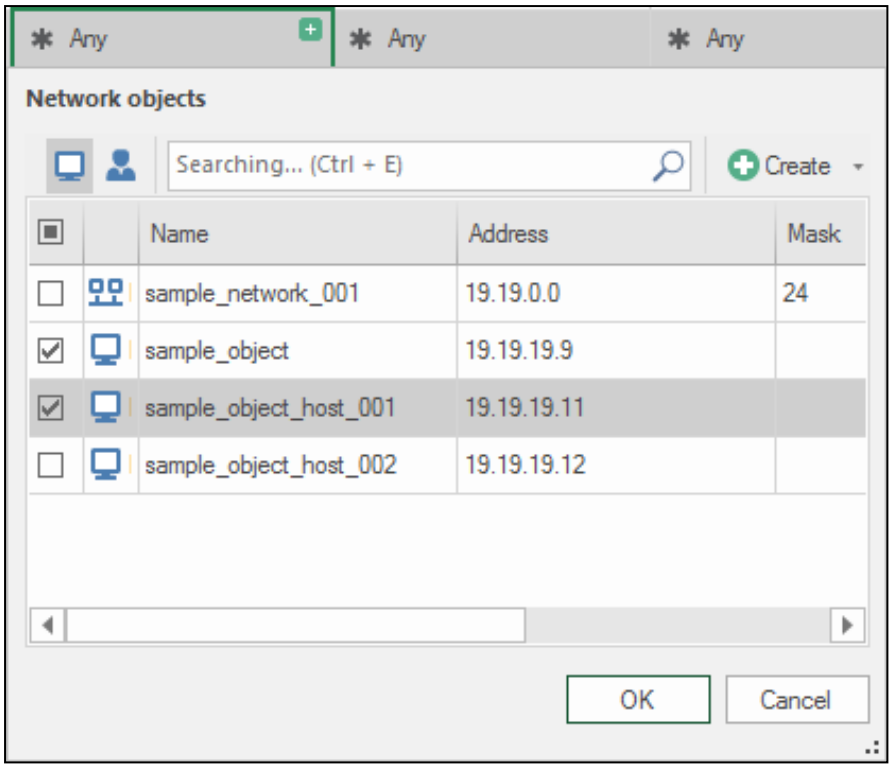
The new rule with an empty name cell and default parameter values appears in the table.

There are the following rule parameters:

- Name;
- Filter:
  - Source;

    Attention!
    Only network objects of the Security Management Server can be set in the **Source** parameter.
  - Destination;
  - Service;
  - Traffic Classifier;
  - Transferred, MB;
- Action:
  - Remark — adding a ToS byte to IP packet headers (an IP packet must correspond to the QoS rule);
  - Priority;
- Time;
- Log;
- Install On;
- Description.

3. In the new rule, specify the rule parameters using the text boxes and drop-down lists in the parameter cells.



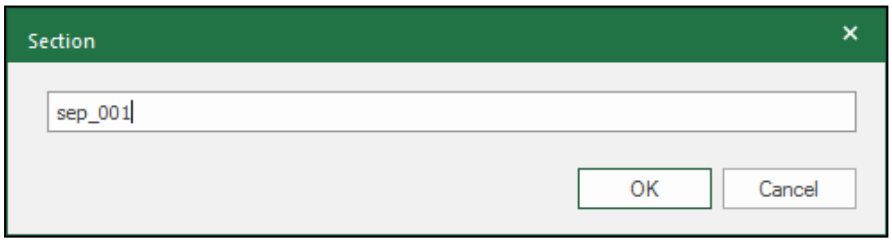
You can sort QoS rules using sections in the rule list.

To sort QoS rules:

1. In the Configuration Manager, go to **Access control** | **QoS**.
2. In the list of rules, select a rule that you want to add to a section.

Note.
The section row is added above the selected rule or the first of the selected rules.

3. Click **Section** on the toolbar, enter the section name and click **OK**.



The created section appears in the list.

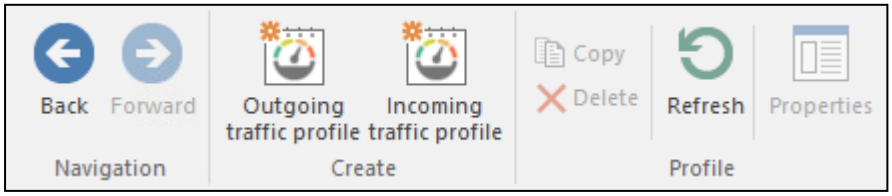
4. Repeat step **2** if necessary.

Create QoS profiles

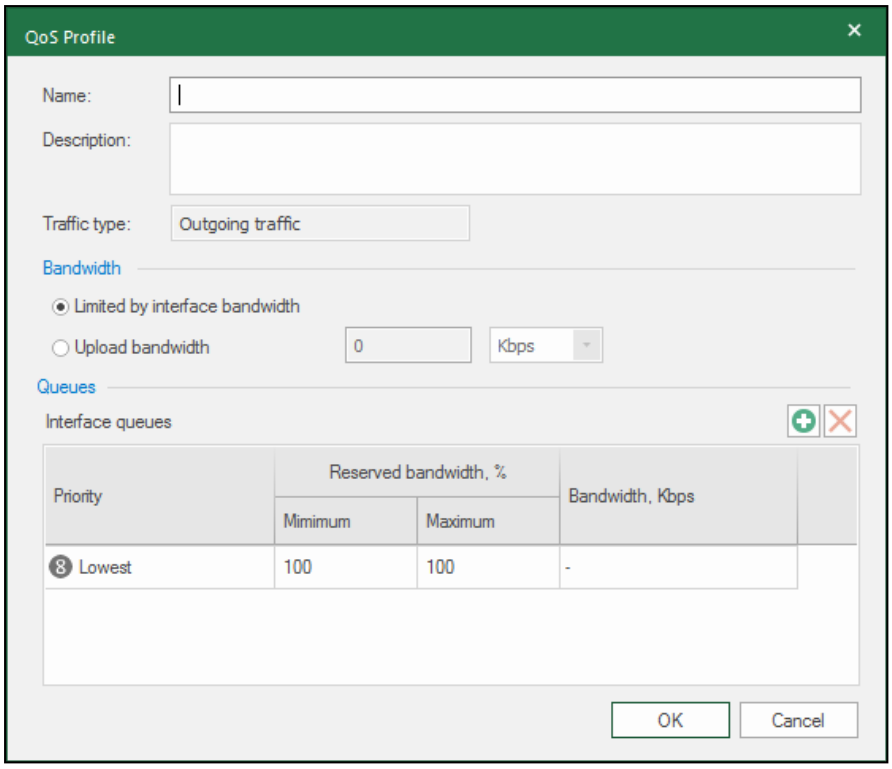
Profiles are created separately for outgoing and incoming traffic.

To create a QoS profile for outgoing traffic:

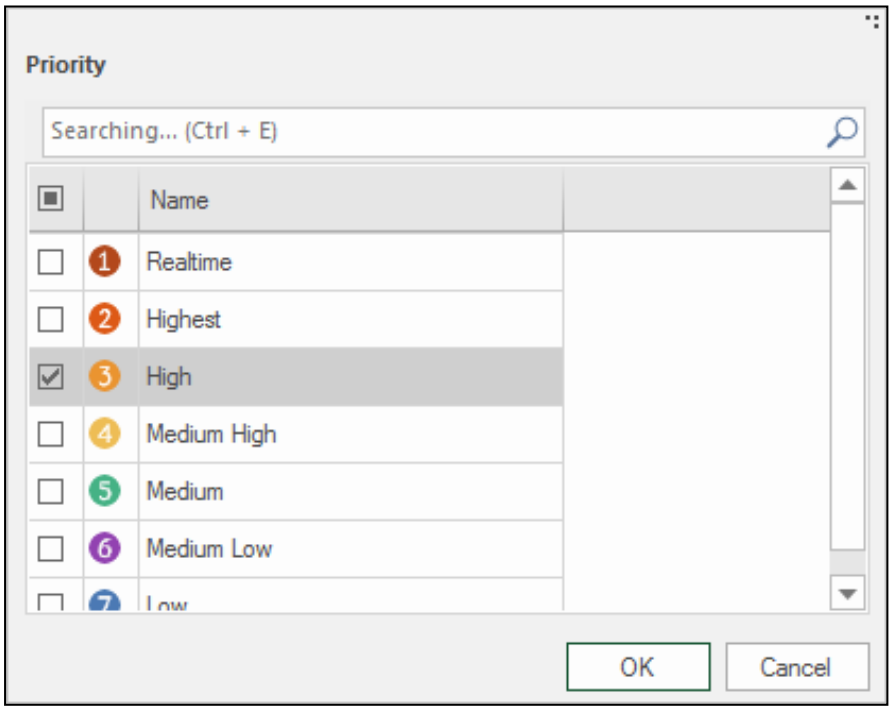
1. In the Configuration Manager, go to **Access control** | **QoS** | **QoS profiles**.
2. On the toolbar, click **Outgoing traffic profile**.



The **QoS Profile** dialog box appears.

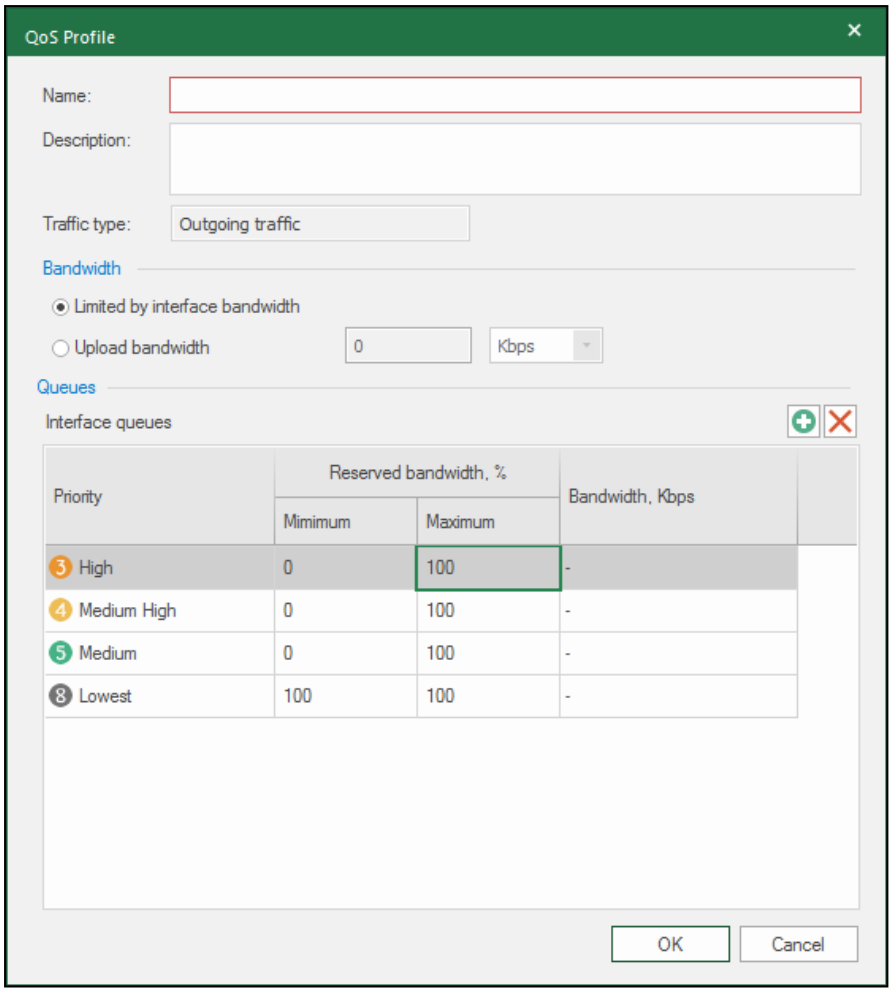


3. Specify the profile name and its description if necessary.
4. In the **Bandwidth** group box, select a bandwidth limitation type.
5. To add an interface queue, click in the **Queues** group box.
   The list of priorities appears.



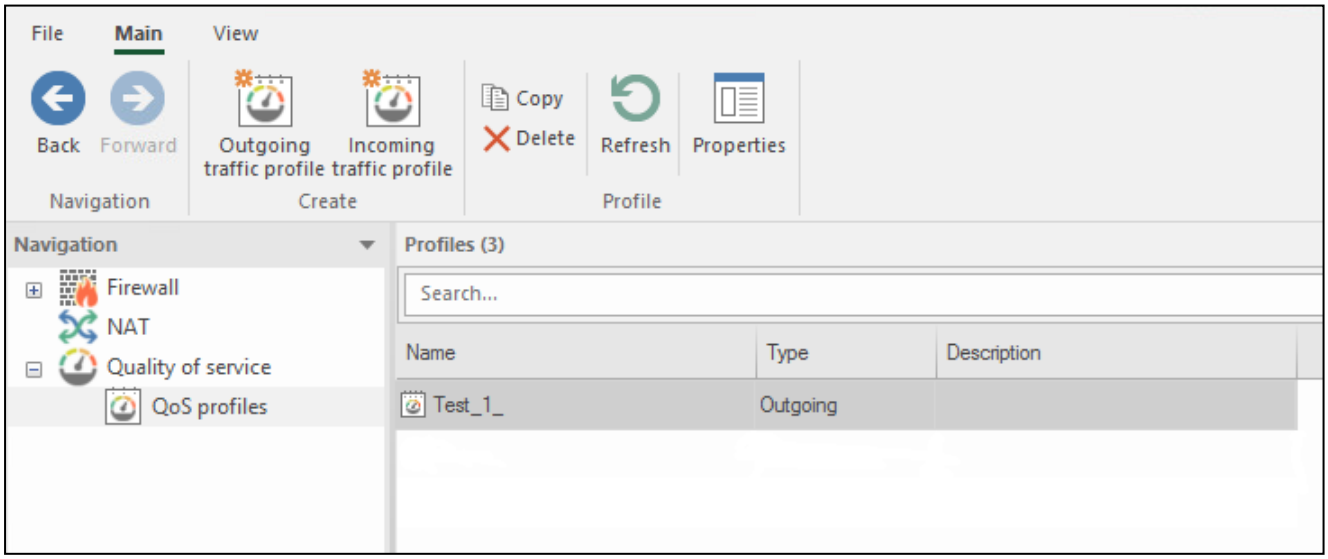
6. Select a priority or priorities in the list and click **OK**.

The queues with selected priorities appear in the list.



7. Specify channel bandwidth limitation for queues if necessary. To do so, enter the required values in the **Minimum** and **Maximum** cells.
8. Click **OK**.

   The created profile appears in the list.

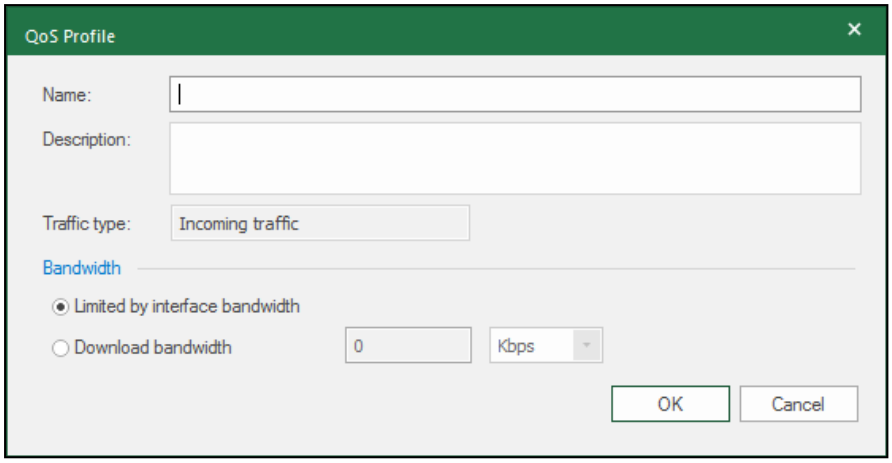


9. If necessary, add another QoS profile for outgoing traffic.

To create a QoS profile for incoming traffic:

1. In the Configuration Manager, go to **Access control** | **QoS** | **QoS profiles**.

2. On the toolbar, click **Incoming traffic profile**.
3. Specify the profile name, its description (if necessary) and select its bandwidth limitation type.

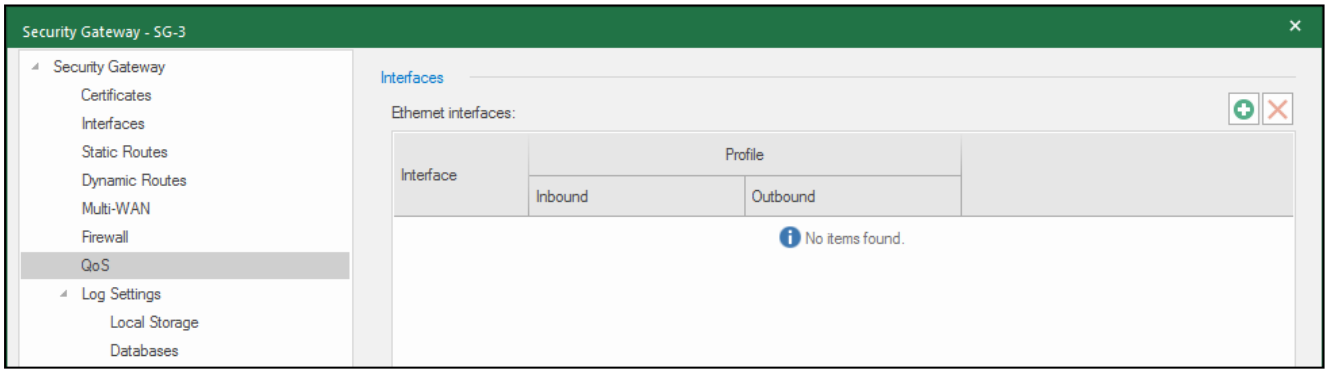


4. To save the profile, click **OK**.
   The created profile appears in the list.

You can assign the created traffic prioritization profiles to Security Gateway interfaces.

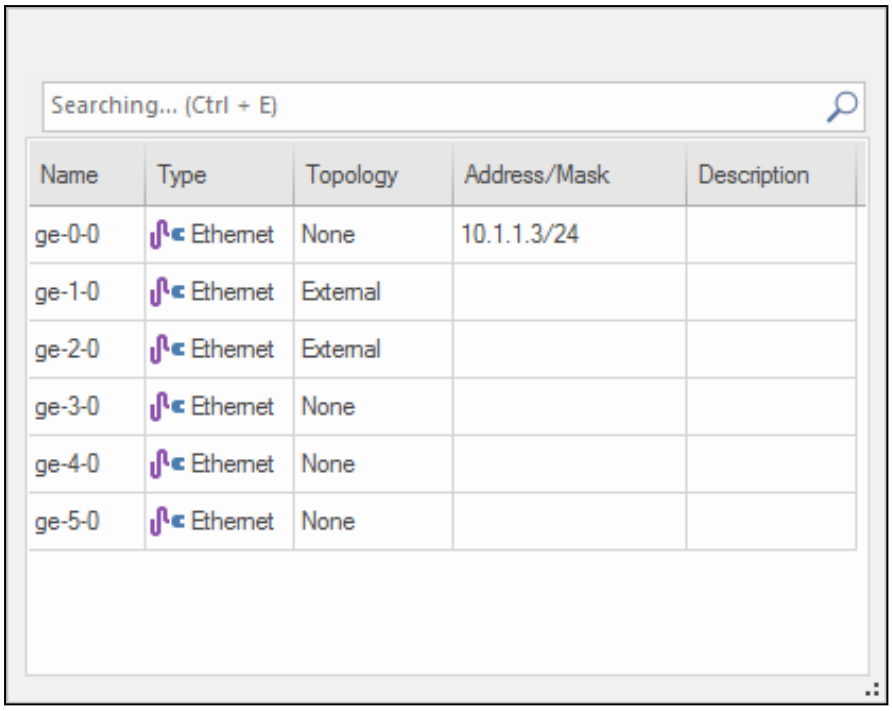
To assign a profile to a Security Gateway interface:

1. In the Configuration Manager, go to **Structure**, select the required Security Gateway with the enabled QoS component and click **Properties** on the toolbar.
   The Security Gateway properties dialog box appears.
2. On the left, select **QoS**.
   The list of profiles assigned to Security Gateway interfaces appears on the right.
   If there are no profiles assigned to the interfaces, the list is empty.

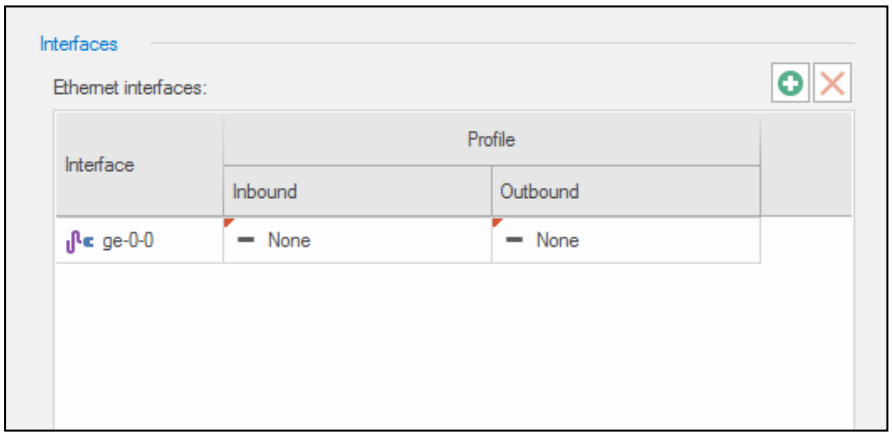


3. Click  .

The list of Security Gateway interfaces available for assigning QoS profiles appears.

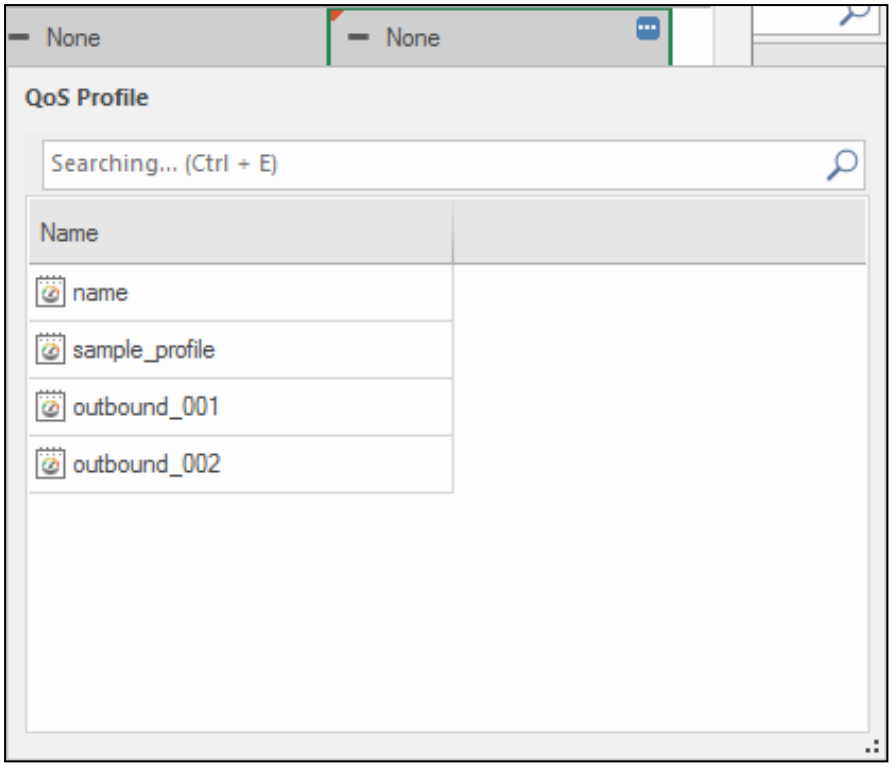


4. Select the required interface.
   The selected interface appears in the list. Inbound and outbound traffic profiles are not specified by default.

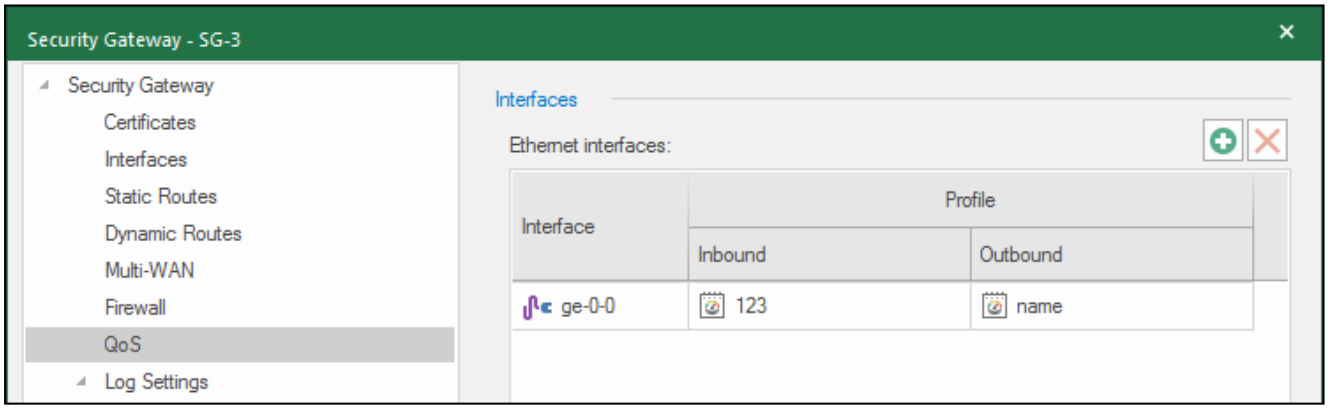


5. Move the pointer over the cell with the required type of QoS profile (**Inbound** or **Outbound**).
   The pop-up button appears in the top right corner of the cell.
6. Click  .

The list of QoS profiles appears.



7. Select the required QoS profile.
   The selected traffic prioritization profile is assigned to the interface.
8. To assign a profile of the other type (**Inbound** or **Outbound**), repeat steps **5**–**7**.
   Inbound and outbound traffic profiles are assigned to the interface.



9. Assign profiles to other Security Gateway interfaces if necessary (repeat steps **3**–**8**).
10. Click **OK**.
    The Security Gateway properties dialog box is closed and you are returned to the Security Gateway list.

DHCP

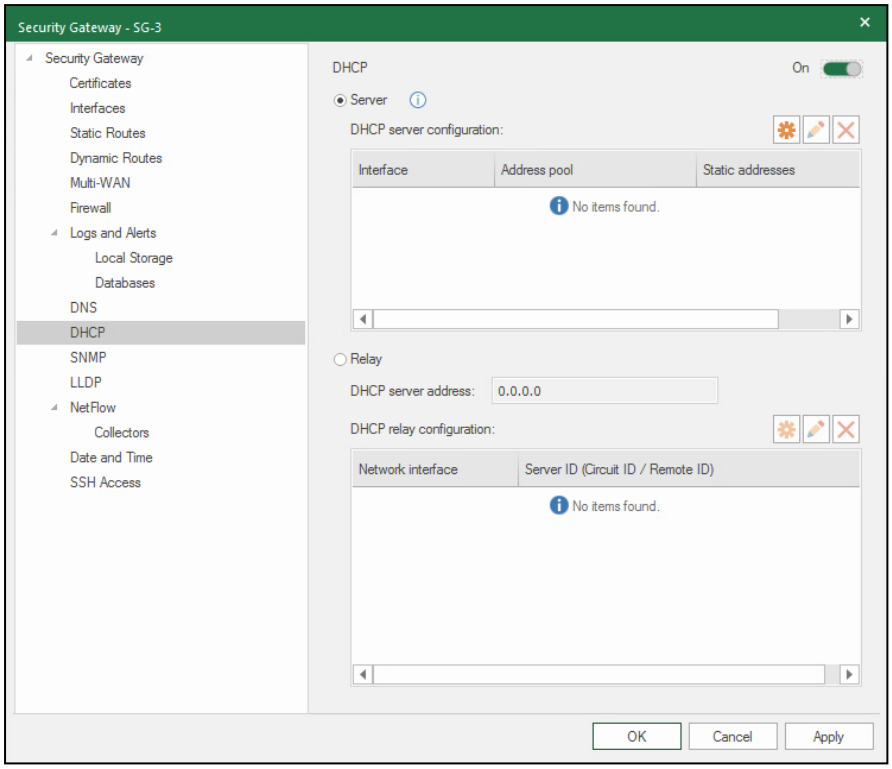
The DHCP mode is disabled after the installation and initialization by default.
You can configure DHCP using the Configuration Manager.

To configure DHCP using the Configuration Manager:

1. Go to **Structure**, select the required Security Gateway and click **Properties** on the toolbar.
   The respective dialog box appears.

2. On the left, select **DHCP**.

   You can see DHCP modes on the right.



For **Server**, there is the list of server profiles. A server profile defines the active internal interface of the Security Gateway and the pool of dedicated addresses.

For **Relay**, specify the IP address of a DHCP server and relay profiles. A relay profile is an internal interface of a Security Gateway on which relay operates and relay parameters of this interface. The relay parameters are:

- Server ID;
- Circuit ID;
- Remote ID.

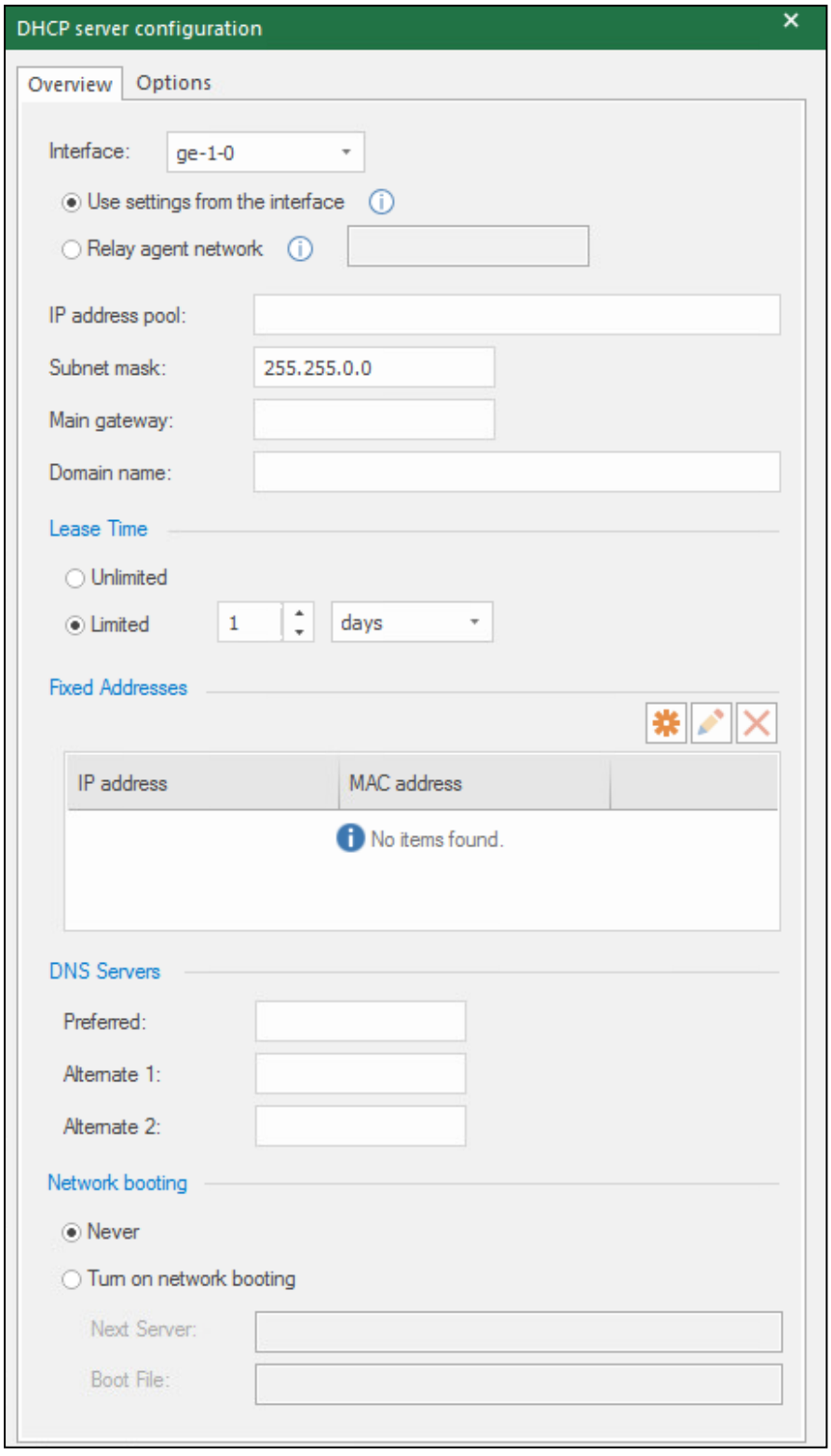
Enable and configure DHCP server mode

To enable and configure the DHCP server mode:

1. In **DHCP**, turn on the toggle.
2. Select **Server**.

   The **Server** parameters become available for editing.
3. To add a new profile, click  .

The **DHCP server configuration** dialog box appears.



4. Select the **Overview** tab.
5. Specify the required DHCP server parameters.

Required parameters	
Interface	The internal interface of a Security Gateway on which the DHCP service operates
Use settings from the interface	A DHCP server and a client are in the same network. A relay is not in use. Enabled by default

Required parameters	
DHCP Relay subnet	A DHCP server and a client are in different networks and have a relay between them. If you select this mode, you need to specify the IP address of DHCP relay network in which it receives client requests
IP address pool	A range of IP addresses
Subnet mask	A mask of a client subnet that includes an IP address pool and a main gateway
Main gateway	An IP address of a used internal interface of a Security Gateway
Domain name	A domain name
Fixed addresses	Permanent IP addresses that are assigned manually, bound to MAC addresses and are not included in the specified address pools
Optional parameters	
Lease time	Lease time of an IP address — 24 hours by default
DNS Servers	Addresses of available DNS servers
Network booting	TFTP server address and a boot file to send through the DHCP server

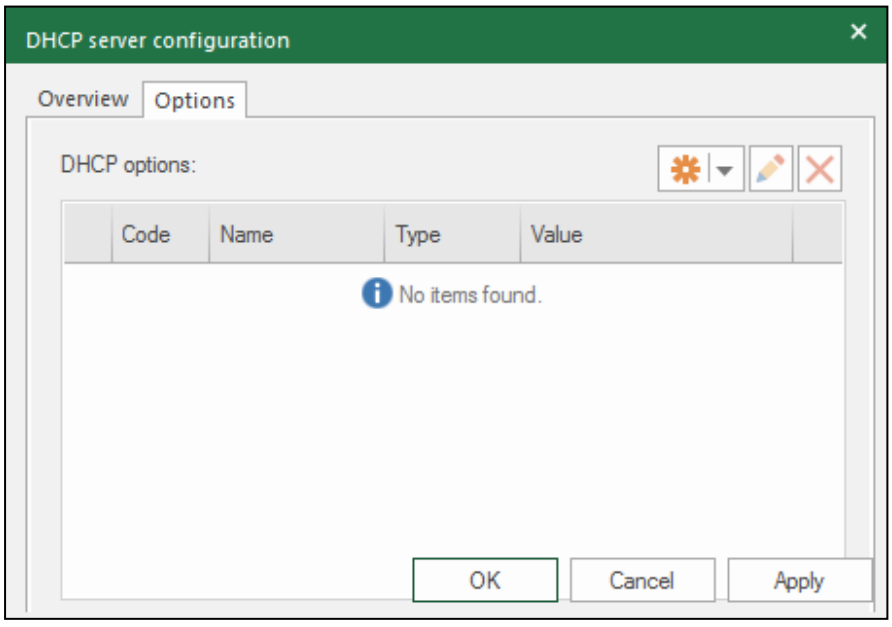
6. Click **OK**.
   The dialog box closes and the parameters appear in the list.
7. If you need to add another profile for another internal interface, repeat step **3**.
8. To edit a profile, click . Make the required changes in the DHCP server configuration and click **OK**.
9. To delete a profile, click .
10. To save changes and finish changing the configuration, click **Apply**.

Configure DHCP server options

Continent provides configuring built-in and custom DHCP server options.

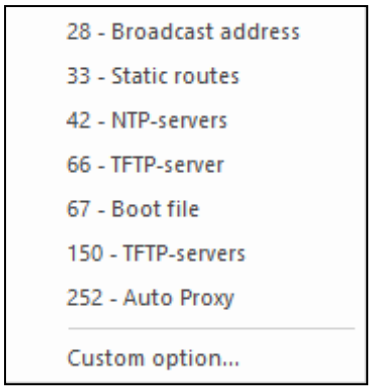
To specify and configure built-in DHCP server options:

1. In the **DHCP** group box, select a profile for which you specify an option and click .
   The **DHCP server configuration** dialog box appears.
2. Go to the **Options** tab.
   The list of DHCP options appears. If no option is specified, the list will be empty.

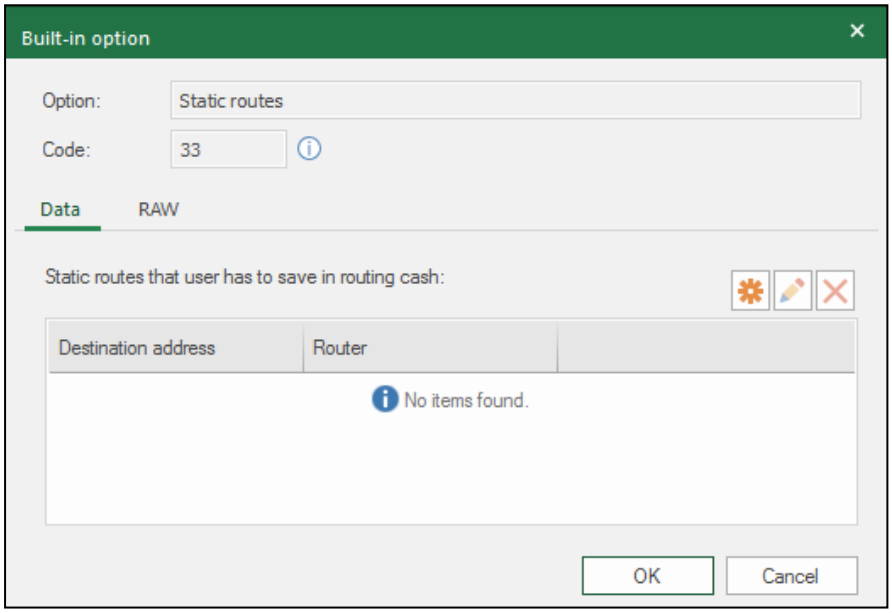


3. Click the arrow located on the right to the button.

The list of the built-in options appears.



4. Select an option.
   The **Built-in option** dialog box appears.



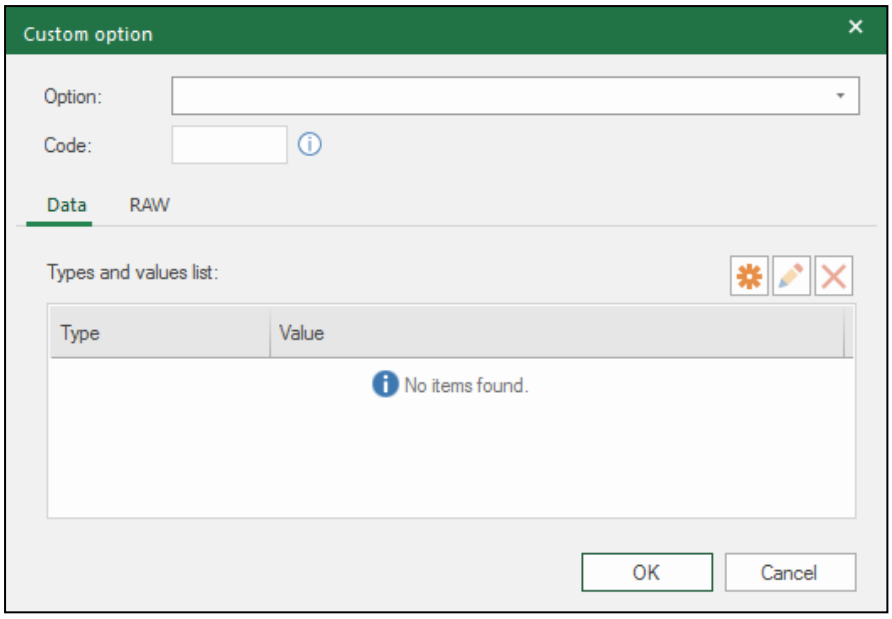
   The **Option** and **Code** fields will be specified automatically.
   The **Data** contents depends on the chosen option.
5. Specify the required values in the **Data** section and click **OK**.
   The option will be added to the list.
6. To add a new built-in option, perform steps **3**–**5**.
7. Click **Apply** to save the configuration.

It is available to configure a custom option (see below).

To add custom options:

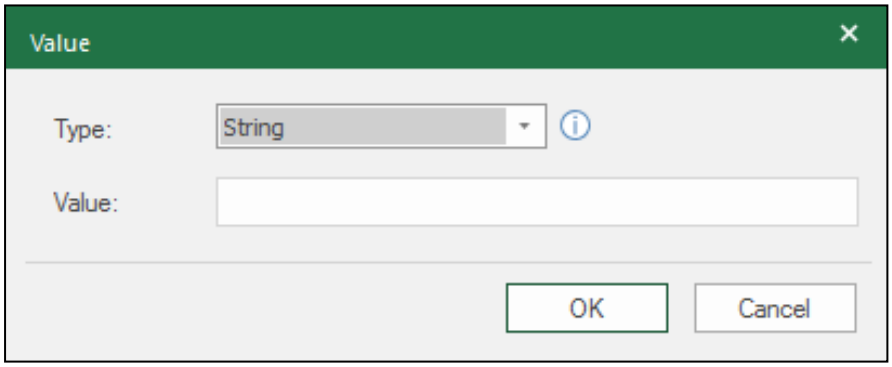
1. In the **DHCP server configuration** dialog box, go to **Options**.
2. Click  and select **Custom option** in the drop-down list.

The **Custom option** dialog box appears.



3. Enter the **Option** and **Code** parameters manually or select them from the list.
4. To do so, click the arrow located on the right to the **Option** field. In this case, the **Option** and **Code** parameters will be specified automatically.
5. In the data section, click .

   The **Value** dialog box appears.



6. In the **Type** drop-down list, select a parameter and specify it in the **Value** text box.
7. Add the required number of options (see steps **2**–**5**).

   To edit the list of custom option types and values, use buttons .
8. Click **OK**.

   The added custom option appears in the **DHCP server configuration** list.

Enable and configure DHCP relay mode

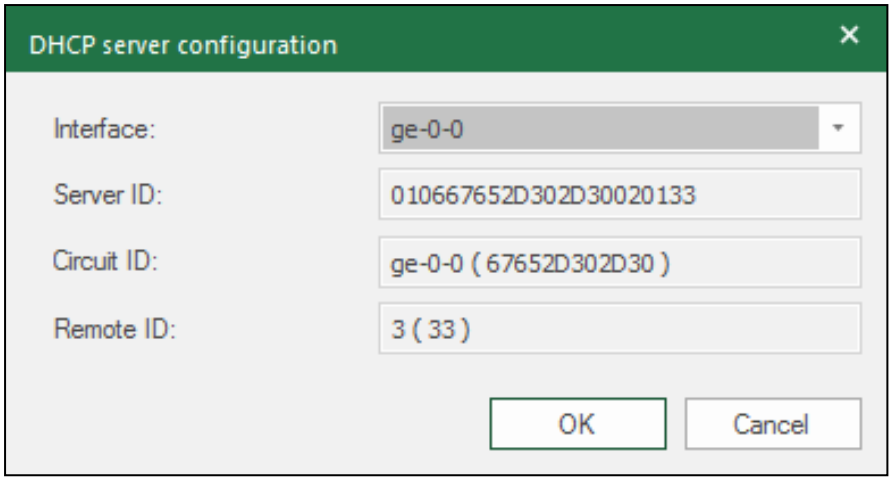
Attention!
Relay is not possible if the DHCP server is in a protected network.

To enable and configure the DHCP relay mode:

1. In **DHCP**, turn on the toggle.
2. Select **Relay**.

   The **Relay** parameters become available for editing.
3. Specify **DHCP server address**.
4. To add a relay configuration, click .

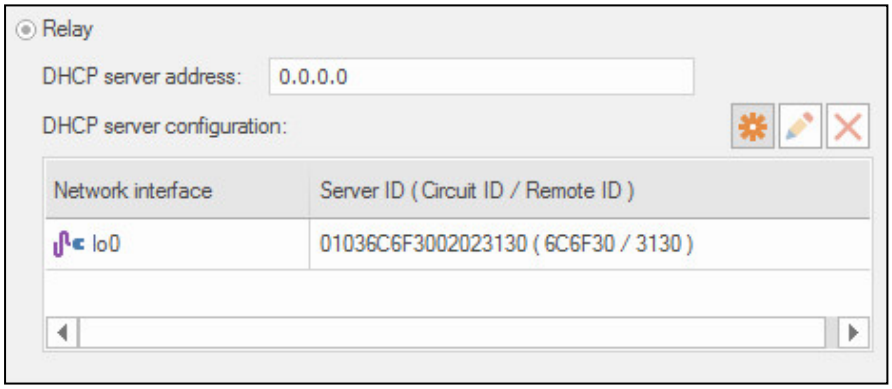
   The **DHCP server configuration** dialog box appears.



5. In the **Interface** drop-down list, select an internal interface.
   After you have selected an internal interface, the other parameters will be specified automatically.

Attention!
When using dynamic routes to access the DHCP server, you need to add an interface towards the DHCP server to the DHCP Relay configuration.

6. Click **OK**.
   The dialog box is closed and the new DHCP relay configuration appears in the list.



7. If you need to add another profile for an internal interface, repeat steps **3**–**6**.
8. To edit a relay configuration, select it in the list and click . Make the required changes and click **OK**.
9. To delete a relay configuration, select it in the list and click .
10. To save changes, click **OK**.

Disable DHCP

To disable DHCP:

1. In **DHCP**, turn off the toggle.
   The **DHCP server configuration** tables of **Server** and **Relay** become unavailable for editing.
2. To save changes and finish configuring DHCP, click **Apply**.

Attention!
- After you have disabled DHCP, all unsaved changes performed earlier will be discarded.
- When excluding a Security Gateway from the cluster with the configured DHCP service, disable the DHCP parameter if it is not supposed to be used.

Time synchronization on Security Gateways

If you want to synchronize the system time using an NTP server, specify its name or IP address. The Security Management Server can operate as an NTP server. The synchronization is performed every hour. You can also

create a list of external accurate time servers. In this case, the most accurate of them is selected automatically.

Attention!

For an NTP server on Windows operating system, the following registry parameters must be set:

- regedit SYSTEM\CurrentControlSet\Services\W32Time\Config\LocalClockDispersion = 0
- regedit SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags = 5

You can configure system time synchronization using both the Configuration Manager and the local menu.

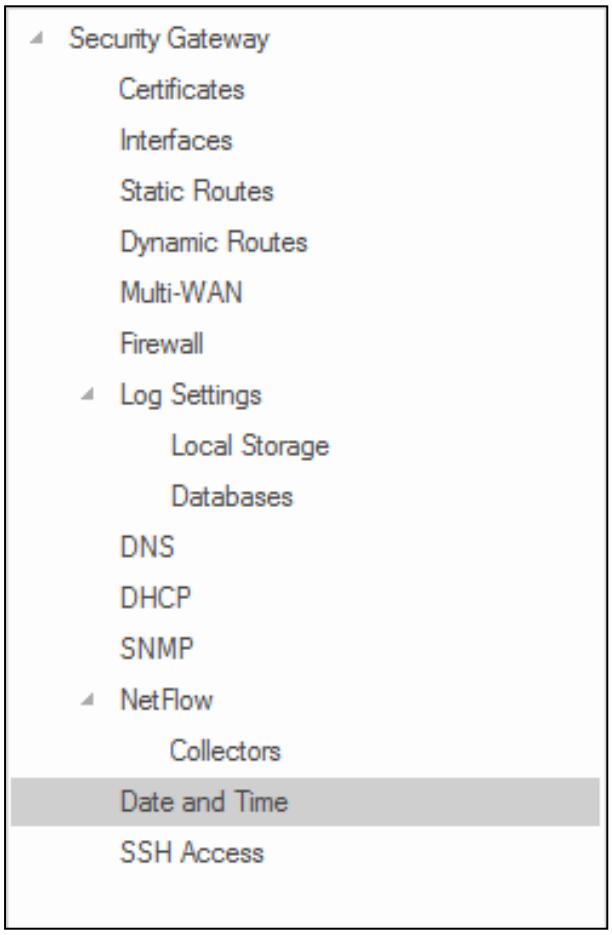
When you send a time synchronization request to a NTP server using the Configuration Manager, the Security Gateway authentication is in use. Authentication is based on a symmetric key mechanism.

The NTP synchronization between the Continent components is enabled by default (Security Gateways automatically synchronize time with the Security Management Server within the domain).

To configure the NTP synchronization of a Security Gateway using the Configuration Manager:

1. In the Configuration Manager, go to **Structure**.
2. Select the required Security Gateway and click **Properties** on the toolbar.

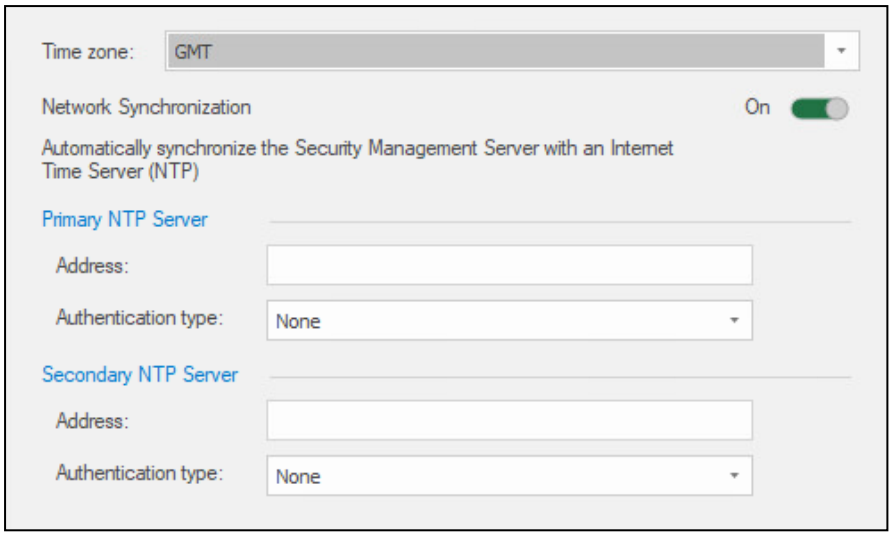
   The Security Gateway properties dialog box appears.
3. On the left, select **Date and Time**.



   The respective settings appear on the right.

   If the **Network Synchronization** check box is not selected, the respective parameters are unavailable.
4. Specify the time zone in the respective drop-down list if necessary.
5. Turn on the **Network Synchronization** toggle.

The synchronization modes are now available.



6. If you are using the Security Management Server as an NTP server, select the respective option button and click **OK**.

   The Security Gateway properties dialog box closes and you are returned to the Security Gateways list.

   Go to step **16**.

7. If you are using an external NTP server, select the **Use Network Time Protocol (NTP)** option button.

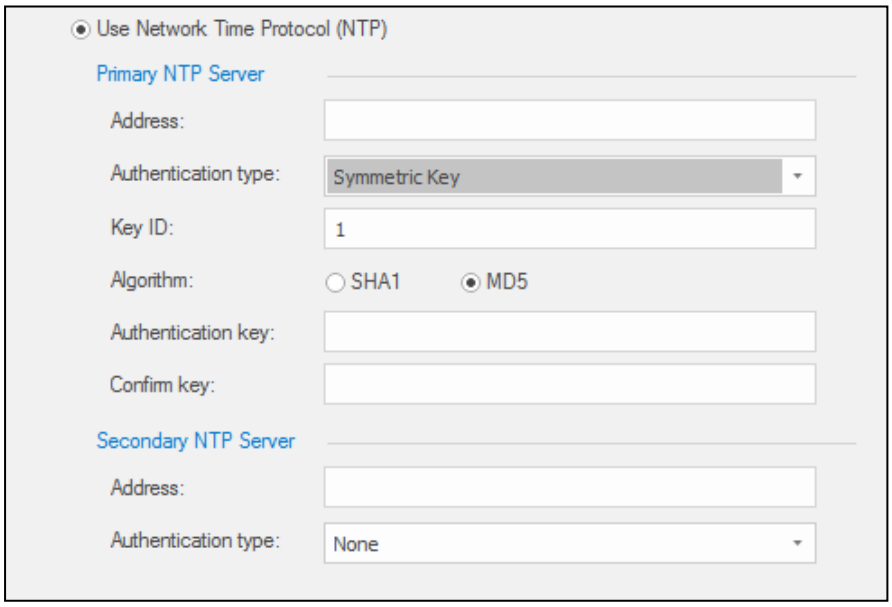
   The NTP parameters are available for editing.

8. Enter the IP address or domain name of the primary NTP server in the respective text box.

9. If the authentication is not required, leave the default **None** value in the **Authentication type** drop-down list and go to step **14**.

10. If the authentication is required, select **Symmetric Key**.

    The NTP server authentication parameters become available.



11. Enter the key ID received from the NTP server administrator in the respective text box.

12. Specify the hash algorithm — **MD5** or **SHA1**.

13. Enter the key received from the NTP server administrator and confirm it in the respective text boxes.

14. Enter the IP address or domain name of the secondary NTP server in the respective text box and configure its synchronization (see steps **9**–**13**).

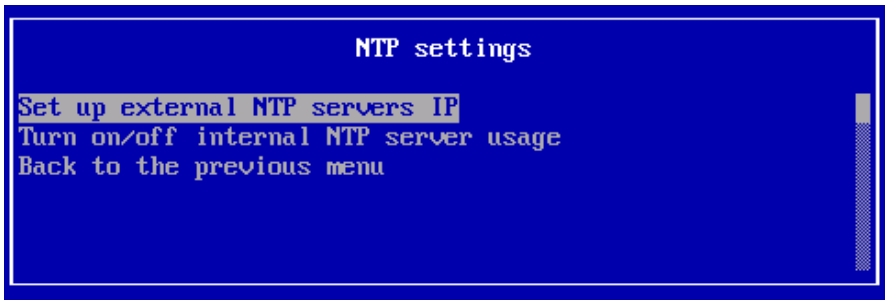
15. Click **OK**.

    You are returned to the Security Gateways list.

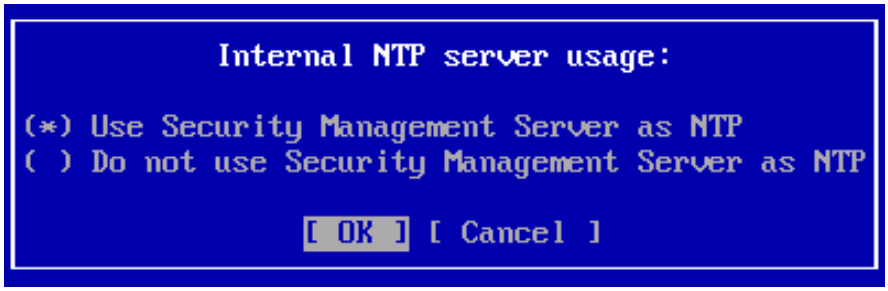
16. Save the changes in the Security Management Server database and install a policy on the Security Gateway.

To configure system time synchronization using the local menu:

1. In the main menu of the required Security Gateway, select **Settings** and press **<Enter>**.
   The **Settings** menu appears.
2. Select **System time** and press **<Enter>**.
   The **Time settings** menu appears.
3. If NTP synchronization is turned off, select **NTP configuration** and press **<Enter>**.
   The **NTP settings** menu appears.



4. If you want to use the Security Management Server as an NTP server, select **Turn on/off internal NTP server usage**.
   The respective dialog box appears.



5. If you need to use the Security Management Server as an NTP server, select the respective option.
   If you need to use an NTP server, select **Do not use Security Management Server as NTP**.
   Select **OK**.
   You will be returned to the previous menu.
6. To configure the NTP synchronization using other servers and to specify their IP addresses, select **Set up external NTP servers IP** and press **<Enter>**.
   The **NTP servers settings** dialog box appears.

7. Enter the addresses of NTP servers, press **<Enter>** and go back to **Settings menu**.
8. To confirm changes, select **Apply local policy** in **Settings** menu and press **<Enter>**.
   Wait for the operation to complete.
9. In the Configuration Manager, go to **Structure**, select the respective Security Gateway and click **Confirm changes** on the toolbar.

Remote access via SSH

To grant remote access privileges to the administrator:

Note.
To configure remote access via SSH, use TCP port 22.

1. In the Configuration Manager, go to **Administration**, select **Roles** and create a new role by clicking the respective button on the toolbar (see [**5**], **Manage administrator roles**).
2. Save changes in the active configuration of the Security Management Server by pressing **<Ctrl>**+**<S>**.
3. To add a created role to an administrator, select **Administrators** on the navigation panel, then select the required administrator or create a new one (see [**5**], **Manage accounts**).

   Note.
   For the built-in administrator, you cannot add a role. Thus, you cannot configure remote access for the built-in administrator.
4. Go to the **Roles** tab of the selected administrator and add the role created in step **1** and click **OK**.
5. To configure using the local management tools, go to step **6**.

   To configure using Configuration Manager, go to step **12**.
6. In the local menu of the Security Gateway to which you want to configure remote access, select **Settings** and press **<Enter>**.

   The respective menu appears.
7. Select **Network** and press **<Enter>**.

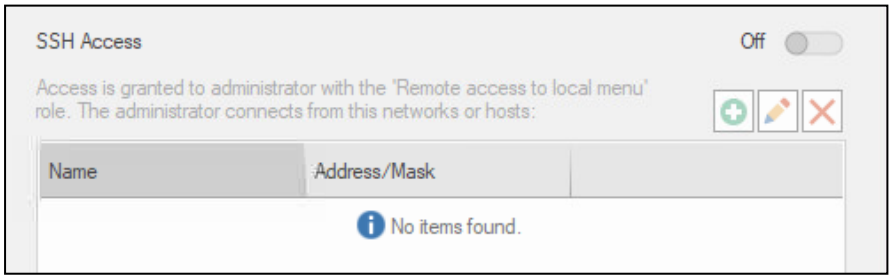
   The respective menu appears.
8. Select **SSH settings** and press **<Enter>**.

   The respective menu appears.
9. Select **SSH access restrictions** and press **<Enter>**.

   The list of IP addresses and subnets with access to SSH service appears.
10. Enter IP addresses from which SSH access is allowed and press **<Enter>**. The maximum number is **10**.
11. Apply the local policy and send the changes to the Security Management Server.

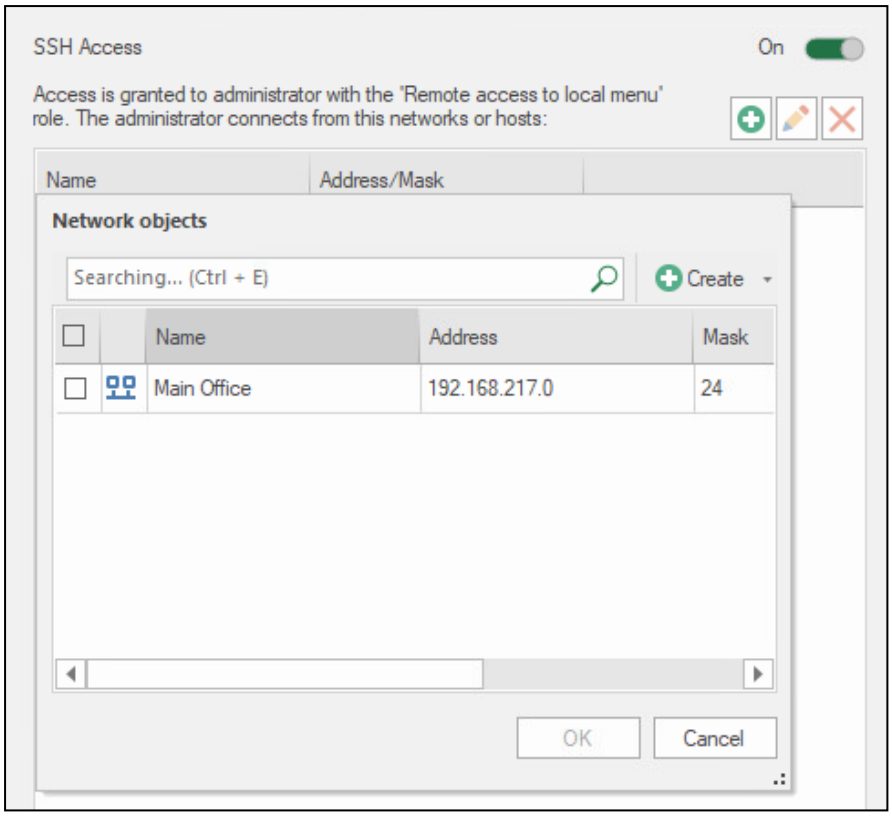
    Attention!
    The configuration made in the local menu is temporary and is valid until the policy is set from the Configuration Manager. Therefore, it is necessary to duplicate the setting in the Configuration Manager as described in this procedure and install the policy on the Security Gateway.
12. To configure using Configuration Manager, go to the **Properties** of the Security Gateway to which local menu you want to configure access via SSH.
13. On the left, go to **SSH**.

    The list of SHH settings appears on the right.



    By default, access via SHH is disabled.
14. Turn on the **SHH Access** toggle and click .

The list of network objects appears on the screen.



15. Select the required objects in the list and click **OK**.

> **Note.**
> If you do not have the required network objects, you can create them. To do this, in the list of network objects, click **Create** or the arrow on the right.

Selected objects will be displayed in the SSH access configuration window.

16. If it is necessary to edit the list of objects, use , , or buttons.

17. Apply the local policy and send the changes to the Security Management Server.

To disable remote SSH access:

- In the Configuration Manager, in the Security Gateway properties window to which you want to disable access, turn off the **SSH Access** toggle, save the changes, and install the policy on the Security Gateway.
- From the local Security Gateway menu, go to **Settings** | **Network** | **SSH settings**, select **Incoming SSH connections**, and then select **Disable incoming SSH connections**. Go back to the **Settings** menu and apply the local policy.

Export data over NetFlow

Overview

In Continent, there is a mechanism that exports data about network traffic that passes through Security Gateways as a flow. This mechanism provides third-party applications with network traffic analysis.

There are the following NetFlow components:

- **Sensor** — selects network data traffic, forms a flow structure and exports stream data to its collector;
- **Collector** — receives data about a flow from a sensor and stores them for further analyzer processing;
- **Analyzer** — processes stored data about flows to provide them to an operator in a required form.

Usually, a sensor is a respective switch device but sometimes it can be a standalone appliance. A sensor can provide one or more collectors with flow data over UDP.

Collector and analyzer are usually a single device that also processes network traffic. To receive data about flows, a collector uses the **2055**, **9555**, **9995** ports.

In Continent, a Security Gateway can operate as a sensor.

According to the settings, an export module can select the following traffic types:

- **transit** — traffic which source and destination are hosts in the protected network;
- **incoming** — traffic which source is a host outside the protected network and destination is a Security Gateway;
- **outgoing** — traffic which source is a Security Gateway and destination is a host outside the protected network.

There are the following export protocols supported:

- Netflow v5 — proprietary Cisco format;
- Netflow v9 — proprietary Cisco format;
- Netflow v10 / IPFIX — open format.

The module sends exported flow data to all the collectors in the list using their address details. In this case, Ethernet/IP/UDP/NetFlow are in use.

If you select the **Export of NetFlow records** check box, the structure of transferred flow data includes the following fields:

Field	IANA IPFIX ID	Description
protocolIdentifier	4	Transport protocol number
sourceTransportPort	7	Source port
sourceIPv4Address	8	Source IPv4 address
destinationTransportPort	11	Destination port
destinationIPv4Address	12	Destination IPv4 address
destinationIPv6Address	28	Destination IPv6 address
vlanID	58	VLAN ID
sourceIPv6Address	128	Source IPv6 address
postNATSourceIPv4Address	225	Translated source IPv4 address
postNATDestinationIPv4Address	226	Translated destination IPv4 address
postNAPTsourceTransportPort	227	Translated source port
postNAPTdestinationTransportPort	228	Translated destination port
natOriginatingAddressRealm	228	Address realm
natEvent	230	Event type
ingressVRFID	234	VRF ID
postNATSourceIPv6Address	281	Translated source IPv6 address
postNATDestinationIPv6Address	282	Translated destination IPv6 address
timestamp	323	Event registration time
portRangeStart	361	Port range start
portRangeEnd	362	Port range end
portRangeStepSize	363	Port range step size
portRangeNumPorts	363	Number of ports in a range

The export module events (enabling, disabling, modification of parameters) are registered in the management log.

Configure export over NetFlow

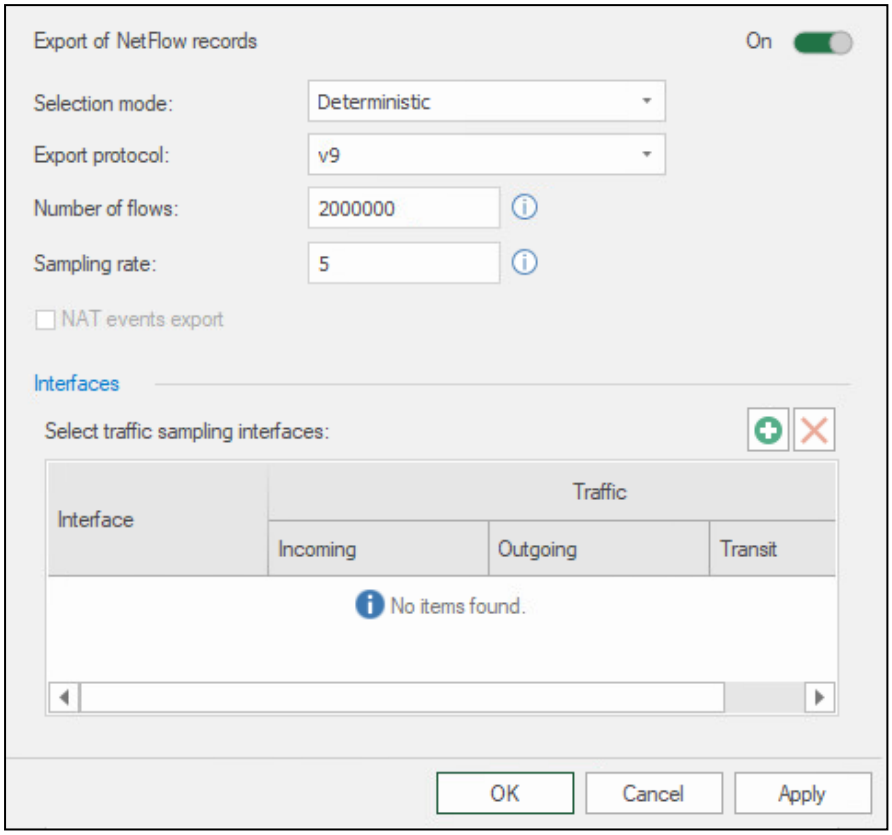
Only main or network administrators can configure NetFlow export.

To configure NetFlow export:

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, select **NetFlow**.
   The respective parameters appear on the right.



3. Turn on the **Export of NetFlow records** toggle.
   The parameters below become available for editing.
4. Specify the following export parameters:

Parameter	Description	Value
Selection mode	Mode of selecting flow data from network traffic	Deterministic
		Random
		Hash
Export protocol	The version of NetFlow protocol used to export flow data	v5
		v9
		v10/IPFIX
Number of flows	The maximum number of flows considered when selecting data from network traffic (to prevent DoS attacks). Integer. Maximum value — **2,000,000**	
Sampling rate	The number of flows selected from network traffic according to the set selection mode. Integer. Maximum value — **16,383**	
NAT events export	A parameter for managing NAT information included to flow data structure. Only for v10/IPFIX	

5. In the **Interfaces** group box, click to specify the interfaces required to process traffic.
   The list of interfaces appears.
6. Select the required interface.
   The selected interface appears in the list.
7. For each interface, specify the traffic type required to select:
   - **Incoming**;
   - **Outgoing**;

- **Transit**.

8. Click **Apply**.
9. On the left, select **Collectors**.

   The respective parameters appear on the right.
10. Click to add a collector.

    A new row appears in the table.
11. Specify the address, port and short description (optional) in the respective cells.
12. Add other collectors if necessary.

    The maximum number of collectors is **5**.
13. Click **OK**.
14. Save the changes and install a policy on the Security Gateway.

Access over ICMP

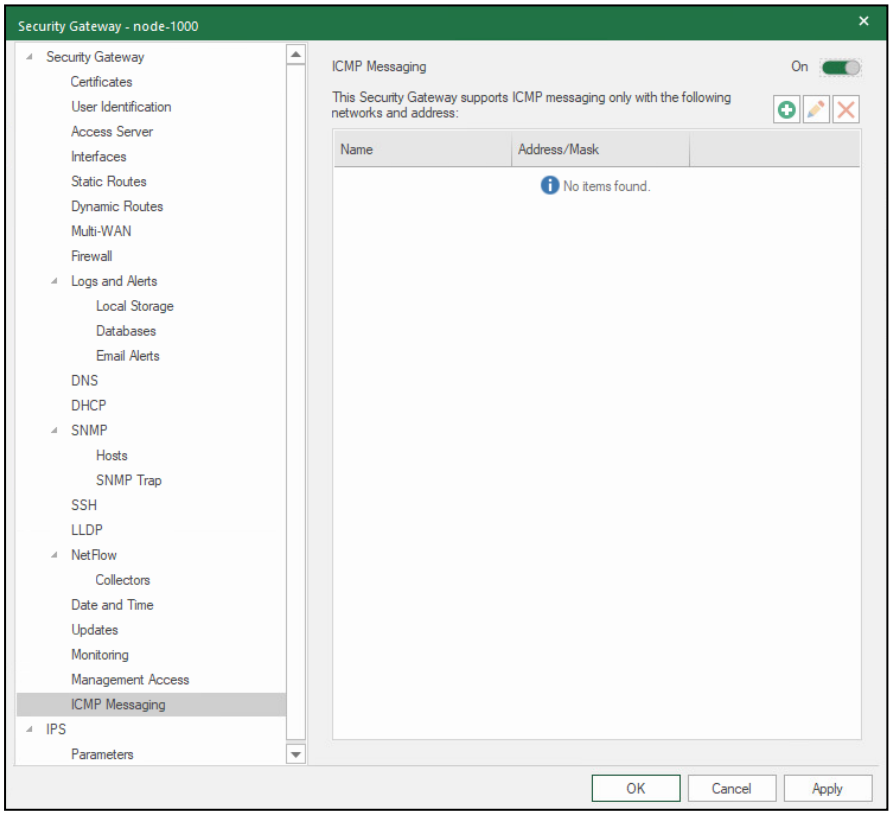
In Continent, there is a mechanism allowing the administrator to monitor access to the Security Gateway over the ICMP protocol ("ping" the Security Gateway).

The administrator can configure hosts, subnets, ranges and groups of IP addresses with which the Security Gateway can exchange messages via the ICMP protocol.

To configure ICMP communication:

1. Select the required Security Gateway and click **Properties** on the toolbar.
2. On the left, select **ICMP messages**.

   The respective parameters appear on the right.



3. To enable the exchange of ICMP messages, turn on the **ICMP messaging** toggle.

   An option to add network objects with which ICMP messaging can be allowed will appear. If the list of network objects is empty, messaging is restricted.
4. Click to add a network object.

   A standard dialog box to select network objects appears.
5. Select the required network objects and click **OK**.

Network objects allowed to exchange ICMP messages with this Security Gateway will be displayed in the **ICMP messaging** list.

6. Save the configuration and install a policy on the Security Gateway.

Collect data on neighboring network devices

Continent enables network devices to receive information about the presence and characteristics from other network devices located in the same network and, in turn, send the same information about themselves. The LLDP protocol is used for data exchange.

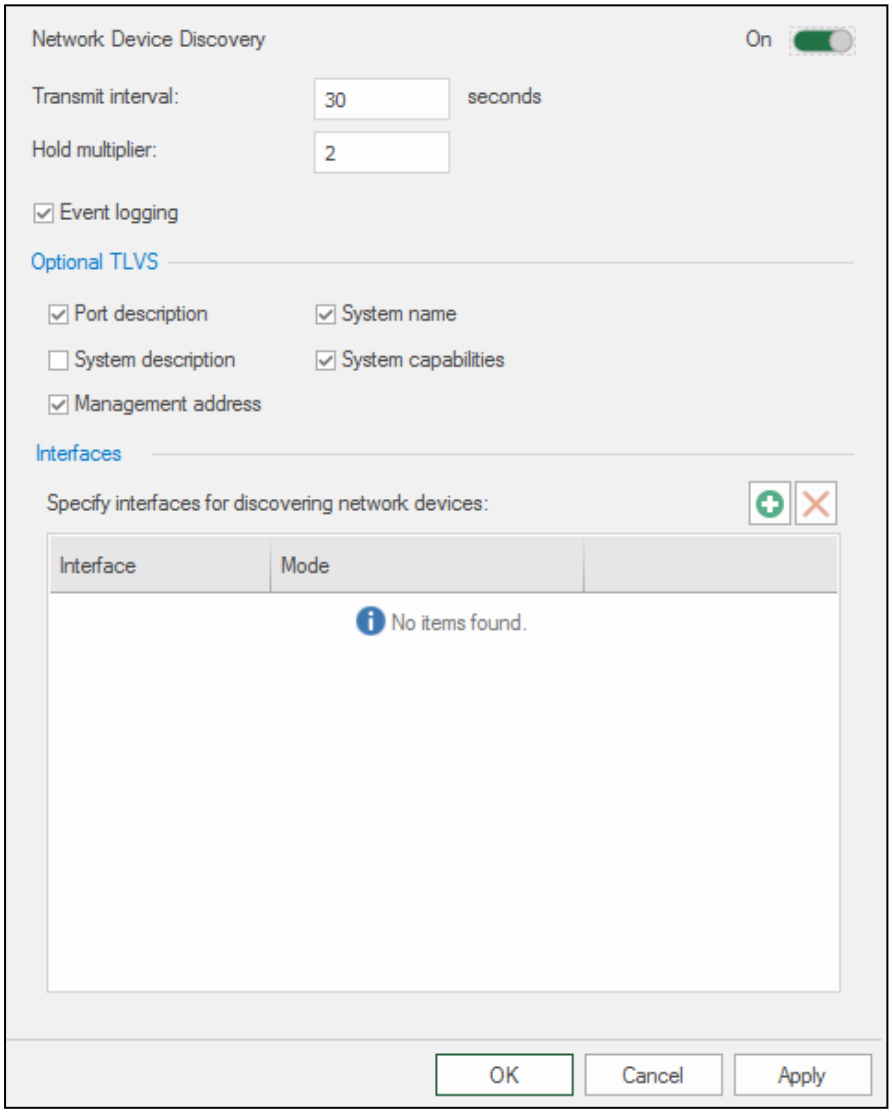
Access to the received data on the neighboring devices is granted under the SMTP protocol. The collected data are displayed in the Continent monitoring subsystem.

The detection mechanism of the neighboring network objects is configured in the Configuration Manager, in the Security Gateway properties (**Configuration Manager** | **Structure** | **Security Gateway** | **Properties**), in **LLDP**.

To configure the neighboring network objects detection mode:

1. In the Configuration Manager, select the required Security Gateway and click **Properties** on the toolbar.
2. On the left, select **LLDP**.

   The **Network Device Discovery** section appears.



   If the LLDP component was not configured earlier or was disabled, the **Network Device Discovery** parameters will be unavailable.

3. Turn on the **Network Device Discovery** toggle.

   The **Network Device Discovery** parameters become available for editing.

4. Specify the general detection parameters:
   - **Transmit interval** (seconds) — time period of sending data on Security Gateways to the neighboring devices.
   - **Hold multiplier** — a parameter that defines the lifetime together with the transmit interval (TTL). TTL is the product of multiplication of the transmit interval and hold multiplier.
5. If the event registration of network devices detection under the LLDP protocol is required, select **Event logging**.
6. In **Optional TLVS**, select the required options if additional data on Security Gateways are to be sent to the neighboring network objects.
7. In **Interfaces**, add the interfaces that detect neighboring network objects by clicking  .
8. For each interface, specify an operation mode: **Receive**/**Transmit**/**Receive and transmit**.
9. Click **Apply** and **OK** consistently after configuring the required parameters.
10. Save the Security Management Server configuration.
11. Install the policy on the Security Gateway.

Appendix

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

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Basics.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Deployment.
3. Continent Enterprise Firewall. Version 4. Administrator guide. Firewall.
4. Continent Enterprise Firewall. Version 4. Administrator guide. Intrusion Prevention System.
5. Continent Enterprise Firewall. Version 4. Administrator guide. Management.
6. Continent Enterprise Firewall. Version 4. Administrator guide. Monitoring and Audit.
7. Continent Enterprise Firewall. Version 4. Administrator guide. VPN.
8. Continent Enterprise Firewall. Version 4. Administrator guide. SNMP.