



Continent Enterprise Firewall Version 4

VPN

Administrator guide



© SECURITY CODE LLC, 2023. All rights reserved.

All rights to operation manuals are reserved.

This document is shipped along with the product kit. It is covered by all terms of license agreement. You may not copy this document in printed or electronic form, in whole or part, or deliver it to third parties on commercial purpose without a special written consent of Security Code LLC.

Security Code LLC reserves the right to change the information contained herein without special notice.

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	5
Introduction	6
VPN concept	7
VPN tunnel	7
Encryption	8
Topology	8
Firewall	8
Licenses	9
VPN deployment	10
VPN deployment procedures	10
Create Security Management Server objects	11
Security Gateways	11
Network objects	12
Configure interfaces	13
Firewall rules	16
Create a Firewall rule	17
Configure a VPN	17
Test VPN operability	19
VPN with cryptographic accelerator	20
Cryptographic accelerator	20
Cryptographic accelerator in full-mesh VPN topology	20
Encryption with pre-checking Firewall compliance	20
Encryption without pre-checking Firewall compliance	22
Cryptographic accelerator in star VPN topology	22
Encryption without pre-checking Firewall compliance	23
Encryption with pre-checking Firewall compliance	25
Model scheme for using Security Gateways in VPN	26
Examples of using the cryptographic accelerator in the model scheme	27
Access from a protected subnet to resources of other subnets	27
Access to corporate resources	32
Configuration for star VPN topology	35
L2VPN deployment	40
Overview	40
Configure L2VPN	40
Configure network interfaces	41
Virtual switches	42
View the list of virtual switches	42
Create a new virtual switch	43
Delete a virtual switch	45
Configure parameters of a virtual switch	45
Model scheme of using L2VPN	46
Model scheme 1	46
Model scheme 2	46
Model scheme 3	46
Model scheme 4	47
Configure data transfer from L2VPN to L3VPN	48
Access to the Internet from L2VPN	49
Connect to a DHCP server from L2VPN	50
Scenarios for using the Security Gateway with the cryptographic accelerator	52
Scenario 1	52
Scenario 2	53
Scenario 3	54
Scenario 4	55
Remote access	56

Overview	56
Access Server	56
Continent-RA	57
Access control	58
Certificate-based user authentication	58
Access Server management	58
Remote access configuration	59
Certificates	59
User list	60
Configure the Access Server	61
Configure an Access Server security cluster	64
Remote access rules	66
Export Continent-RA profiles	67
Documentation	69

List of abbreviations

CSP	Cryptographic Service Provider
DNS	Domain Name System
FTP	File Transfer Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
NAT	Network Address Translation
RSTP	Rapid Spanning Tree Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRP	Vehicle Routing Problem

Introduction

This manual is designed for administrators of Continent Enterprise Firewall Enterprise Firewall, Version 4 (hereinafter — Continent).

This document contains links to documents [1] – [5].

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 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 4.1.7 — Released on December 5th, 2023.

Chapter 1

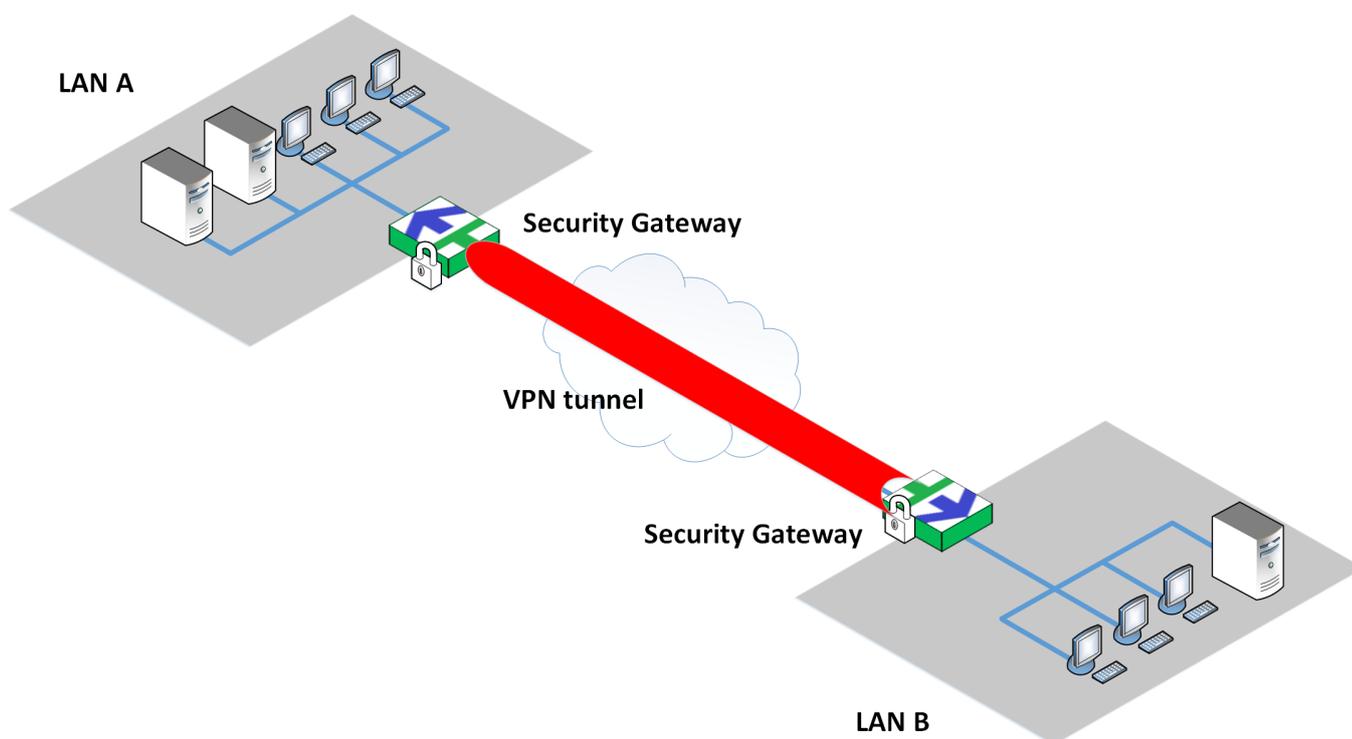
VPN concept

VPN makes it possible to combine LANs, their segments or standalone workstations of a company into a single secure virtual network. The transition from a distributed LAN to a VPN helps you reduce the maintenance costs. However, the creation of a VPN over a public network requires extra protection measures from unauthorized access for corporate information resources.

VPN tunnel

Using Continent VPN, you can create secure channels (tunnels) between two Security Gateways. Each Security Gateway that acts as the Firewall protects a LAN or a network segment. When traffic is transferred from one protected network to another one, it is encrypted before getting into the tunnel and decrypted after getting out of the tunnel.

In the figure below, there are two LANs. Each of them has its own Continent Security Gateway. They are connected using public data networks (for example, via the Internet).



Hosts of the **A** and **B** LANs exchange data using a tunnel between Security Gateways:

1. The Security Gateways are connected to each other and create a tunnel.
2. The **A** host sends packets to the **B** host.
3. The **A** Security Gateway encrypts the packets and sends them through the tunnel.
4. The **B** Security Gateway decrypts the packets and sends the packets to the destination host.
5. The **B** host receives the decrypted data.

Packets are transferred backwards in the same way — when the **B** host starts to exchange data with the **A** host. The packet encryption prevents unauthorized access when a third party intercepts it.

A VPN tunnel does not impose any additional requirements on the **A** and **B** users. Applications on their computers keep generating packets with respective source and destination addresses as usual. Security Gateways perform all operations for encrypting, encapsulating and transferring packets.

Encrypted data is transferred only within the tunnel between two Security Gateways. A host and a Security Gateway exchange unencrypted data.

One Security Gateway can maintain more than one tunnel at the same time and each tunnel can support more than one connection.

Encryption

In Continent, VPN uses symmetric-key cryptography. A connection between Security Gateways is based on the shared secret key mechanism. Each IP packet is encrypted using one packet encryption key based on a shared secret key.

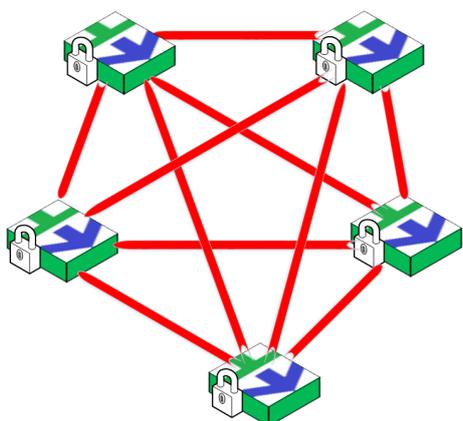
Data encryption meets GOST R 34.12-2018 (Magma) requirements in Cipher Feedback Mode. Message authentication meets GOST R 34.12-2018 (Magma) requirements using a message authentication code.

Topology

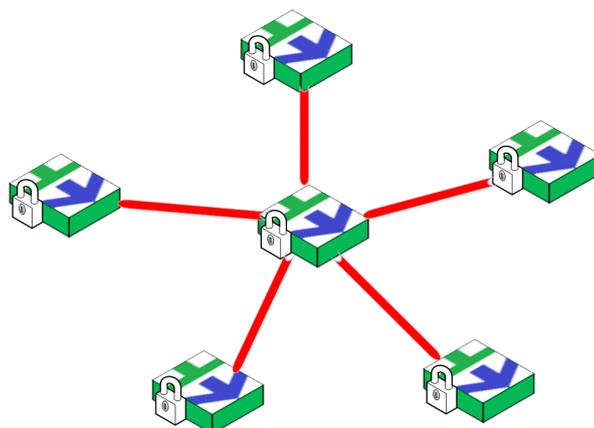
You can create VPN tunnels between Continent Security Gateways and build a single VPN with the **star** or **full-mesh** topology.

In **full-mesh**, tunnels are created for each Security Gateway pair.

In **star**, there is a central Security Gateway. Other Security Gateways can be connected only to the central one.

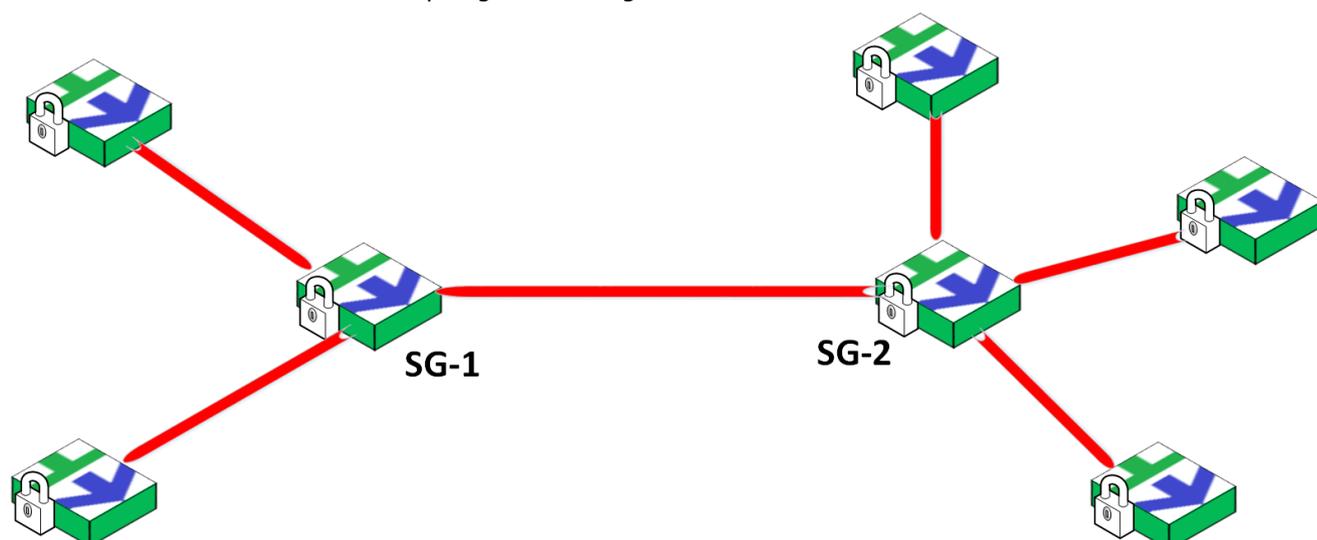


Full-mesh



Star

You can see the mixed use of base topologies in the figure below.



The **1** and **2** Security Gateways form a full-mesh VPN segment, but the both are the central Security Gateways in the star segments.

Firewall

Continent Security Gateways can also operate as a firewall.

For VPN, the Firewall policy describes the following:

- WAN interfaces;
- LAN interfaces;
- VPN operation schedule;
- types of transferred data.

For traffic to pass correctly, you must specify Firewall rules passing traffic on Security Gateways. For more information, see [2].

Licenses

For proper operation, VPN requires valid licenses linked to all Continent Security Gateways transferring traffic.

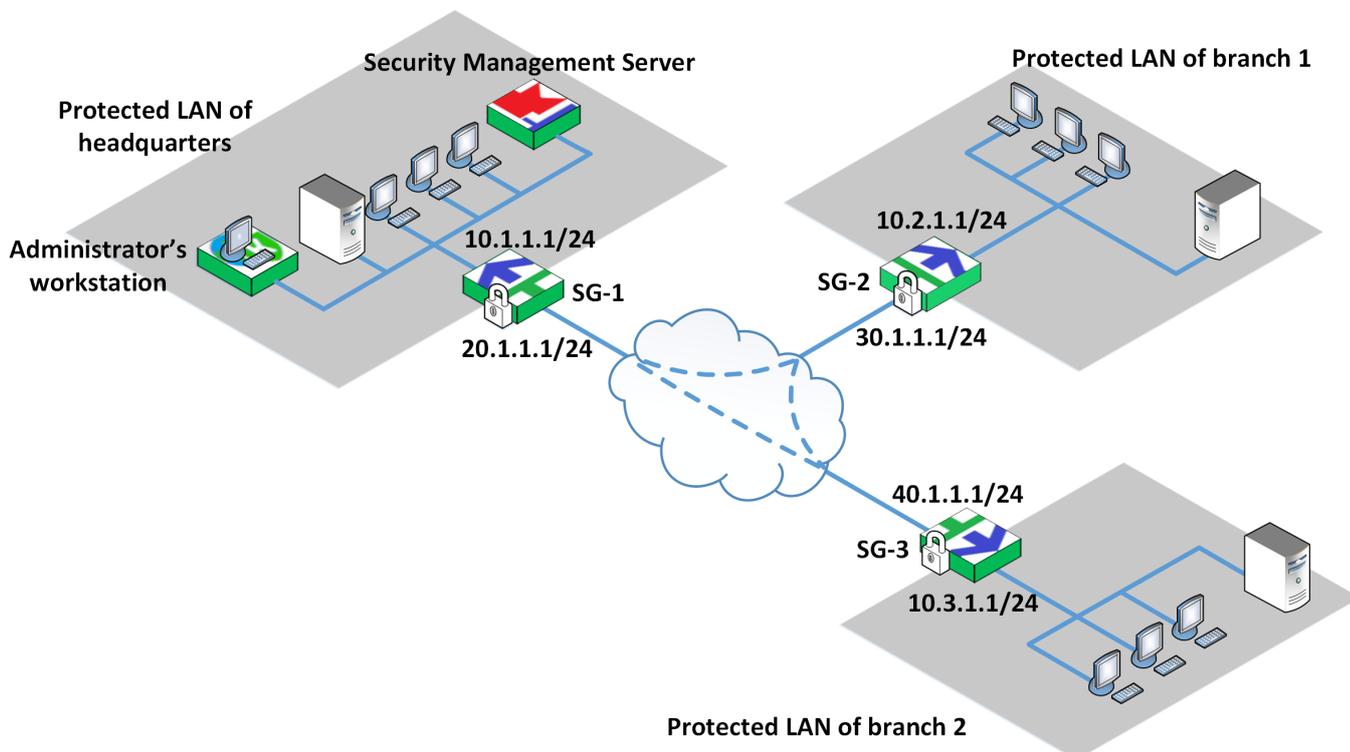
The preinstalled demo license is valid for 14 days and allows you to use L3VPN and L2VPN, and the Access Server with two connections.

For more information, see [1].

Chapter 2

VPN deployment

An example of a corporate VPN connecting its headquarters with two branches is in the figure below.



The VPN contains the following components:

- Security Gateways **SG-1**, **SG-2** and **SG-3**;
- Security Management Server deployed in a protected LAN of the headquarters;
- Configuration Manager installed on the administrator's computer in the protected LAN of the headquarters.

The following IP addresses will be used in the following examples:

SG-1

Interface	IP address/Mask
Internal	10.1.1.1/24
External	20.1.1.1/24

SG-2

Interface	IP address/Mask
Internal	10.2.1.1/24
External	30.1.1.1/24

SG-3

Interface	IP address/Mask
Internal	10.3.1.1/24
External	40.1.1.1/24

VPN deployment procedures

Deployment of a VPN consists of the following steps:

1. Create Security Management Server objects (see below).

2. Configure Security Gateway interfaces (see p. 13).
3. Create Firewall rules (see p. 16).
4. Create a VPN based on the required topology (see p. 17).
5. Check the operability of the configured VPN channels (see p. 19).

Create Security Management Server objects

To create a VPN, you need to create routes and Firewall rules passing traffic within protected networks. Routes and Firewall rules use Security Management Server objects such as Security Gateways and network objects (see detailed information in [2]).

Security Gateways

You create Security Gateways when deploying Continent (see [1]). You can see the list of created Security Gateways in **Structure** of the Configuration Manager and also in an additional area in **VPN**.

See the list of Security Gateways used in VPN configuration on p. 10.

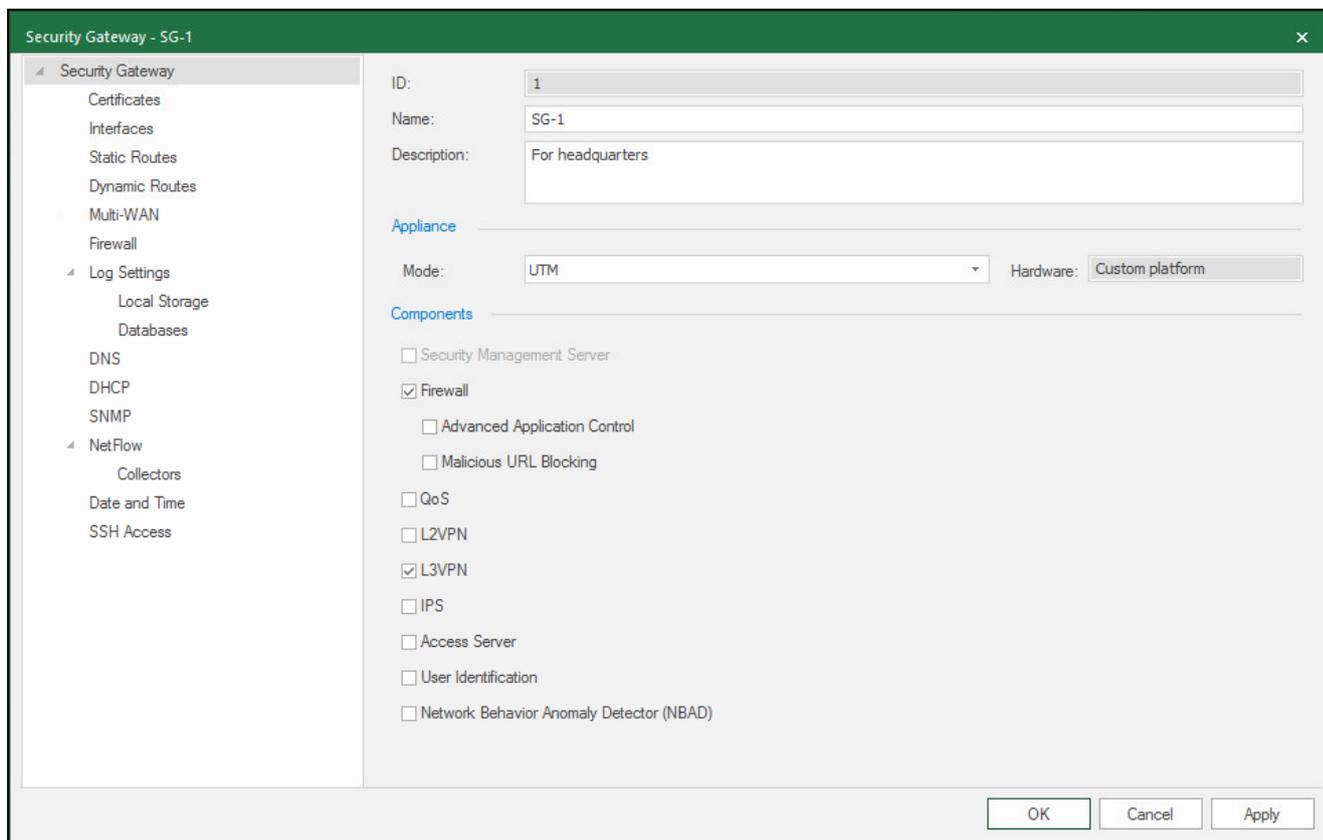
Security gateways (4)						
Search...						
Status	Name	Components	Configuration	Cluster	Certificate validity, days	Description
Online	node-10		10082	-	363	
Online	SG-1		10082		364	
Online	SG-2		10082		364	
Online	SG-3		10082		364	

Note.

When working with lists, the Configuration Manager provides a search for the required list item. The search can be performed by attributes of the element (Security Management Server object, interface, filtering rule, etc.). To do this, enter the attribute value or its part in the **Search** field and press **<Enter>**. Also, you can enter logical expressions containing **and**, **or**, **not**, **()** in the **Search** field.

To view or configure Security Gateway parameters:

1. Right-click the required Security Gateway in the list and select **Properties**.
The respective dialog box appears as in the figure below.



On the left, there is a menu. On the right, you can see the parameters according to the selected menu item. To read about parameters of Security Gateway networking functions, see [3].

2. In the **Components** group box, select **Firewall** and **L3VPN**.

To read about configuration of VPN parameters, see the following chapter.

3. Click **OK** and save the configuration.

Network objects

For traffic to pass from one LAN to another, you need to create three **Network** objects:

- headquarters;
- branch 1;
- branch 2.

You also need to create an **All_Net** group of network objects that includes all the **Network** objects.

The procedures for creating and configuring network objects are described in [2].

To view the list of network objects:

- In the Configuration Manager, go to **VPN**.

The list of network objects appears at the bottom of the display area.

You can see the list of all the network objects mentioned previously in the figure below.

Objects				
<input type="text" value="Search..."/>				
	Name	Address	Mask	Description
	All_Net	-	-	All network objects
	Headquarters	10.1.1.0	24	The protected network of headquarters
	Branch 1	172.17.10.0	24	The protected network of branch 1.
	Branch 2	172.17.9.0	24	The protected network of branch 2.

All_Net includes all the **Network** objects.

Group - All_Net
✕

Overview
Group membership

Name:

Description:

Members:

	Name	Address	Mask
	Headquarters	10.1.1.0	24
	Branch 1	10.2.1.0	24
	Branch 2	10.3.1.0	24

Configure interfaces

Attention!

Network interface names provided in the examples or in the pictures may not coincide with the real ones and may vary depending on the Security Gateway platform.

You must configure interfaces for each Security Gateway.

To configure interfaces:

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

The list of Security Gateways appears in the display area. In the table below, you can see descriptions of the Security Gateways shown in the figure on p. [10](#)

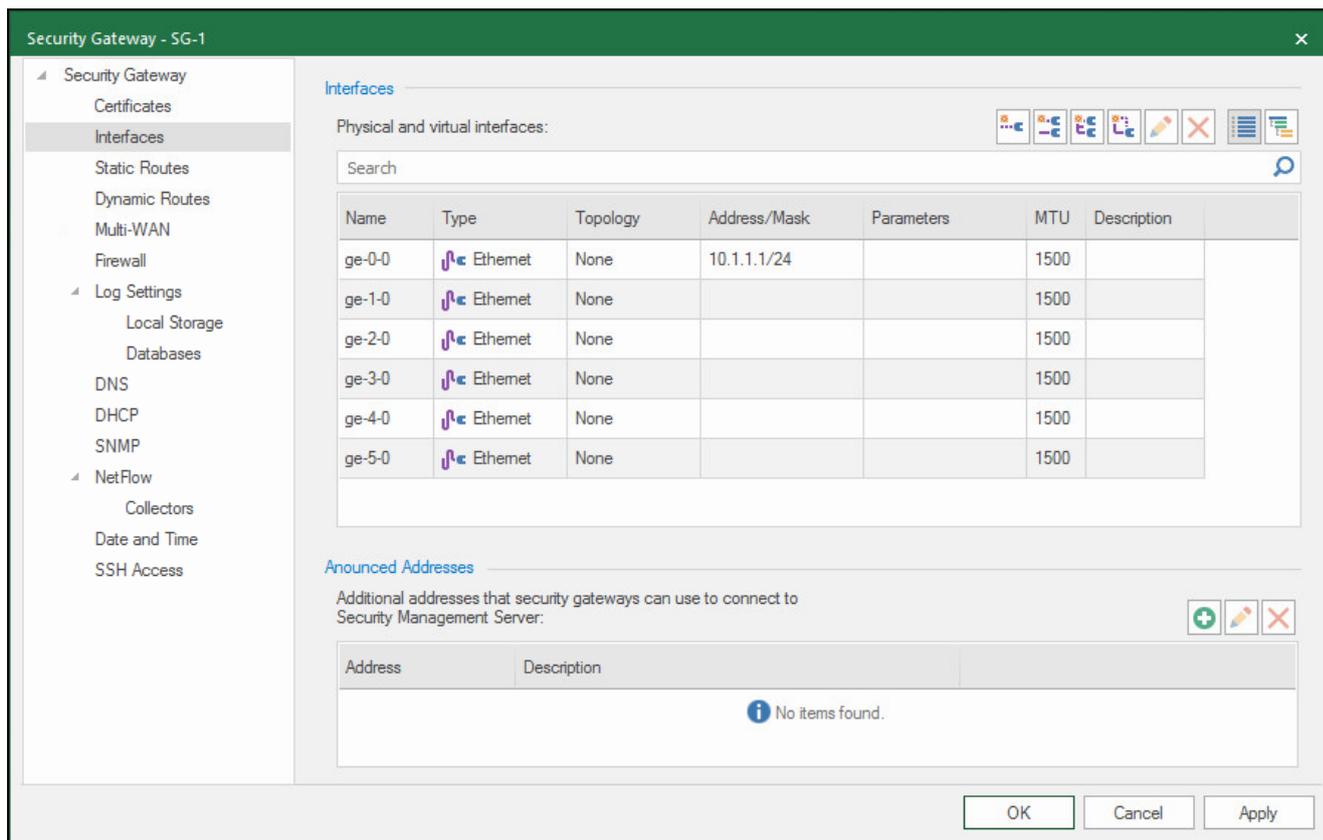
Security Gateway	Description
SG-1	Security Gateway 1 in the headquarters
SG-2	Security Gateway 2 in branch 1
SG-3	Security Gateway 3 in branch 2

2. Right-click the required Security Gateway (for example **SG-1**) and select **Properties**.

The respective dialog box appears.

3. On the left, select **Interfaces**.

The list of Security Gateway interfaces appears.

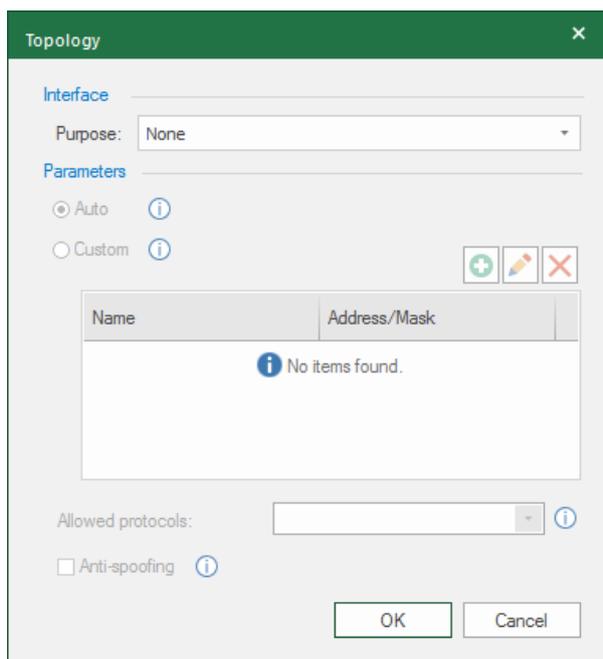


It displays information sent to the Security Management Server after the Security Gateway initialization.

If the interface parameters have not been configured, the parameters will be set by default (see the figure above). The parameters will be set by default (see the figure above).

4. Specify the topology of the used interfaces. Place the cursor in the **Topology** field of the required interface and click the pop-up button.

The **Topology** window appears.



5. In the **Purpose** drop-down list, select the interface purpose and click **OK**.

The **Topology** window will close and the selected value will appear in the field.

6. Specify the IP address and the mask. To do so, select the required cell and select or specify the required value.

7. Specify the purpose of the used interfaces (**Internal** or **External**) and their IP addresses for the second interface.

The following parameters must correspond to the configuration of **SG-1**:

Interface	Topology	Address/Mask
ge-0-0	Internal	10.1.1.1/24
ge-1-0	External	20.1.1.1/24

8. If necessary, specify other parameters set by default:

- **MTU**;
- **DF bit** (see [5], **Configure DF bit**);

In the **Parameters** field, the procedures for configuring other parameters described in [5] can be started.

9. Click **OK**.

The properties window closes.

10. Repeat all previous steps for **SG-2** and **SG-3** according to the information on p. 10.

11. Save the changes by clicking  in the top left corner of the Configuration Manager.

For the model scheme on p. 10, the following interface parameters of Security Gateways are in use:

SG-1

Interfaces

Physical and virtual interfaces:

Search

Name	Type	Topology	Address/Mask	Parameters	MTU	Description
ge-0-0	Ethernet	Internal	10.1.1.1/24		1500	
ge-1-0	Ethernet	External	20.1.1.1/24		1500	
ge-2-0	Ethernet	None			1500	
ge-3-0	Ethernet	None			1500	
ge-4-0	Ethernet	None			1500	
ge-5-0	Ethernet	None			1500	

SG-2

Interfaces

Physical and virtual interfaces:

Search

Name	Type	Topology	Address/Mask	Parameters	MTU	Description
ge-0-0	Ethernet	Internal	10.2.1.1/24		1500	
ge-1-0	Ethernet	External	30.1.1.1/24		1500	
ge-2-0	Ethernet	None			1500	
ge-3-0	Ethernet	None			1500	
ge-4-0	Ethernet	None			1500	
ge-5-0	Ethernet	None			1500	

SG-3

Interfaces

Physical and virtual interfaces:

Search

Name	Type	Topology	Address/Mask	Parameters	MTU	Description
ge-0-0	Ethernet	Internal	10.3.1.1/24		1500	
ge-1-0	Ethernet	External	40.1.1.1/24		1500	
ge-2-0	Ethernet	None			1500	
ge-3-0	Ethernet	None			1500	
ge-4-0	Ethernet	None			1500	
ge-5-0	Ethernet	None			1500	

Firewall rules

For traffic to pass from one protected VLAN to another one, you need to create respective Firewall rules using the Configuration Manager. The created rules are stored in the Security Management Server database as a list.

After you install a policy, the Firewall rules are installed on the selected Security Gateways and define the gateway reaction against certain IP packets.

By default, Security Gateways do not pass any IP packets until the administrator has created Firewall rules and installed policies on Security Gateways using the Configuration Manager.

Create a Firewall rule

You can use already created objects of the Security Management Server to create Firewall rules or create them while creating a rule.

To provide communication between hosts of protected networks in headquarters and branches, you need to install a rule passing traffic between the protected networks on each Security Gateway (1–3).

For more information about the creation and application of Firewall rules, see [2].

An example of creating a rule passing traffic is shown in the following procedure, where **All_Net** contains network objects of the headquarters and branches 1 and 2. **All_Net** is also considered the source and destination.

To create a Firewall rule:

1. In the Configuration Manager, go to **Access control** and select **Firewall** on the navigation panel.

The list of Firewall rules appears in the display area.

Note.

If you have not created rules, the list will be empty.

2. On the toolbar, click the required button in the **Create** group. If the list is empty, click any button.

Note.

You can also select the required command by right-clicking the display area.

The created rule appears in the display area.

Sections (0), Rules (1)									
Search...									
No.	Name	Source	Destination	Service	Application	Action	Profile	Install On	
1		* Any	* Any	* Any	* Any	Drop	* None	* All	

3. Set the following parameters:

- Source: **All_Net**;
- Destination: **All_Net**;
- Action: **Accept**;
- Install On: **SG-1, SG-2, SG-3**.

You may keep other parameters as they are.

The created rule with set parameters appears in the display area.

4. Save changes in the Security Management Server database by clicking  on the Quick Access Toolbar.

Sections (0), Rules (1)									
Search...									
No.	Name	Source	Destination	Service	Application	Action	Profile	Install On	
1	VPN	All_Net	All_Net	* Any	* Any	Accept	* None	SG-1 SG-2 SG-3	

Attention!

This rule is an example of Firewall rule passing IP packets between the hosts of the protected networks and can be used only with other Firewall rules.

5. Click **Install policy** on the toolbar.

The respective dialog box appears.

6. Select the required Security Gateways and click **OK**.

The respective task appears in the **Notification center**.

Configure a VPN

When you create a VPN, you need to take the following steps:

- specify a name and a description;

- add all Security Gateways required for the tunnel creation and protected network objects to a VPN;
- select a topology (full-mesh or star).

To create a VPN:

1. In the Configuration Manager, go to **VPN** and select **L3VPN**.

The list of created VPNs appears.

Note.

If there are no created VPNs, the list is empty.

2. On the toolbar, click **VPN**.

The respective dialog box appears.

3. Enter a name and a brief description in the required text boxes, then click **OK**.

The dialog box closes and the created VPN appears in the list.

4. Select it and click **Add Security Gateway** on the toolbar.

The list of all the Security Gateways appears.

5. Select the required Security Gateway.

The Security Gateway is added to the VPN as its member. The VPN becomes full-mesh by default.

Topology	Members	Network objects	Description
ABC	SG-1		

6. Repeat steps 4-5 to add all the required Security Gateways.

7. If you need a star VPN, click  in the **Topology** column and select the respective option.

Topology	Members	Network objects	Description
ABC			

The topology of the VPN will be changed in the list and the icon of the first Security Gateway will be changed to .

8. If you need another Security Gateway to be central, right-click it in the list and select **Set as central Security Gateway**.

9. For each Security Gateway, you can select protected resources if necessary.

To do so, click  in the **Network objects** column and select the required object. If you have not created the required object yet, create it by clicking .

10. Save the changes in the Security Management Server database by clicking  and install the policy on the required Security Gateways.

Test VPN operability

You can test VPN operability using the **ping** utility.

Perform this test for each Security Gateway pair that should be connected with a VPN tunnel. For example, test the operability of the VPN channel between **SG-1** and **SG-3** in a full-mesh VPN (see p. 10).

To test the operability of a VPN tunnel:

1. Start **ping** from the protected network of branch 2 to any host in the protected network of headquarters.
2. In the local menu of **SG-1** or **SG-3**, go to **Tools | Diagnostics | Command line**.
3. In **Command line**, start **tcpdump** with defining the interface: **tcpdump -i te-0-0**.

The information about traffic passed between **SG-1** and **SG-3** appears.

Attention!

If **SG-1** is the central one in a star VPN, there are two VPN tunnels passing traffic: **SG-2–SG-1** and **SG-3–SG-1**. In this case, you need to start **ping** from the protected network from one branch to another and then start **tcpdump** in **SG-1** in order to check encrypted traffic. The result of the test is encrypted packets passing from the external interface of the branch Security Gateway to the external interface of **SG-1** and encrypted packets sent from **SG-1** to the Security Gateway of another branch and vice versa.

Chapter 3

VPN with cryptographic accelerator

The Continent 4 product kit includes hardware that can be integrated with a cryptographic accelerator. A Security Gateway integrated with a cryptographic accelerator operates faster when encrypting VPN traffic.

Cryptographic accelerator

The cryptographic accelerator can:

- encrypt — receive traffic from a secure internal interface, encrypt the contents of a packet, calculate the message authentication code, encapsulate and send packets through the external network interface;
- decrypt — receive traffic from an external interface, decapsulate packets, check the message authentication code and the collation and send packets through a secure internal interface.

The cryptographic accelerator has its own interfaces that can be either internal or external. The external interface is designed to exchange encrypted data with other Security Gateways. The internal interface is designed to connect a device to LAN segments, protected by a Security Gateway. In the Configuration Manager, the cryptographic accelerator interfaces are denoted as ca0–ca3.

A Security Gateway encrypts traffic according to the cryptographic accelerator scenario: packets may be encrypted with or without pre-checking for Firewall rule compliance. The scenario also defines the interface that transfers encrypted packets to a VPN channel: the external interface of a Security Gateway or a cryptographic accelerator. The contents of a scenario depend on a VPN topology (full-mesh or star).

Cryptographic accelerator in full-mesh VPN topology

Encryption with pre-checking Firewall compliance

The figure below illustrates the way of getting access from the secure network **SN0** to the resources of the secure network **SN1**.

SG-1 protects **SN0** as the Firewall with the cryptographic accelerator.

SG-1 receives IP packets via its own internal interface, processes them and sends them to the cryptographic accelerator according to Firewall rules.

The cryptographic accelerator encrypts IP packets, encapsulates them and sends them from the external interface to the VPN channel.

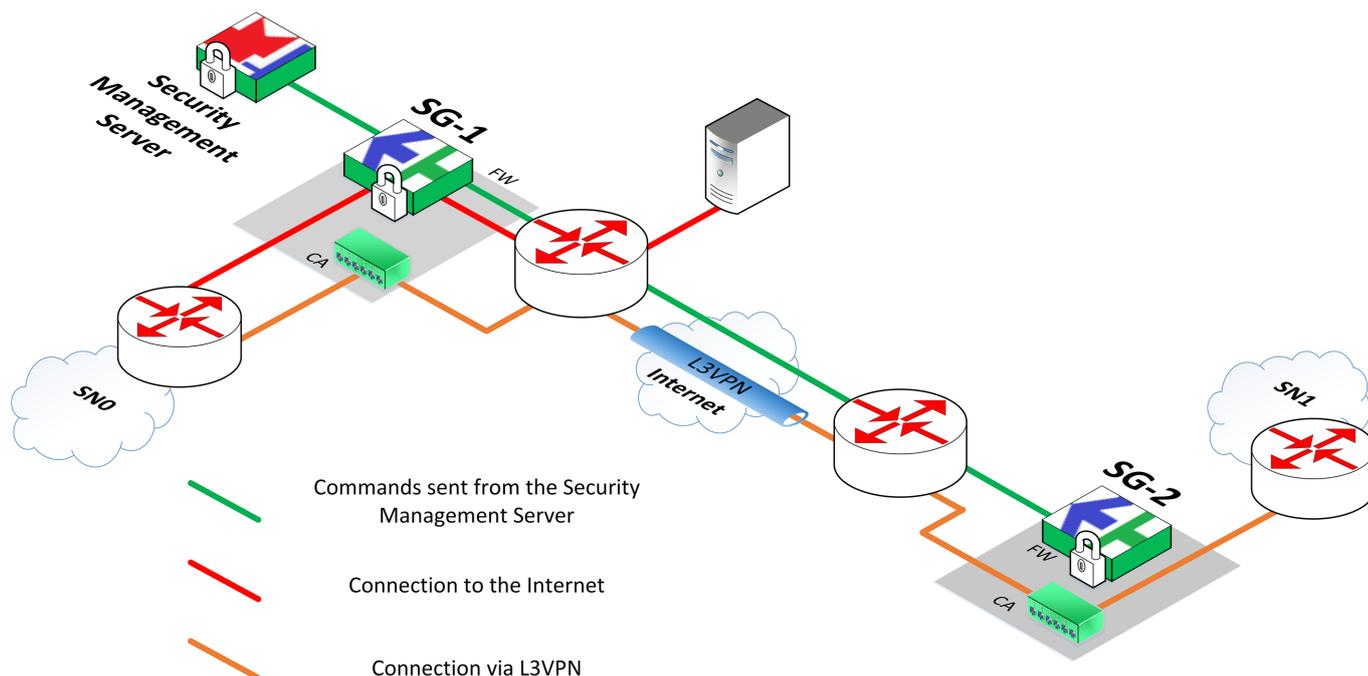
The external interface of **SG-2** cryptographic accelerator receives encrypted IP packets.

SG-2 cryptographic accelerator decapsulates IP packets, decrypts them and sends to **SG-2**.

SG-2 processes decrypted packets according to Firewall rules and sends them from the internal interface to **SN1**.

Encryption without pre-checking Firewall compliance

The figure below illustrates the scenario where **SG-1** encrypts packets without pre-checking Firewall compliance.



The cryptographic accelerators of **SG-1** and **SG-2** create a VPN channel.

The cryptographic accelerator of **SG-1** receives IP packets from **SN0** by its own internal interface, encrypts, encapsulates, then sends them from its own external interface according to the routing tables.

The cryptographic accelerator of **SG-2** receives IP packets by its own interface, decapsulates IP packets, decrypts then sends them from its own internal interface to **SN1**.

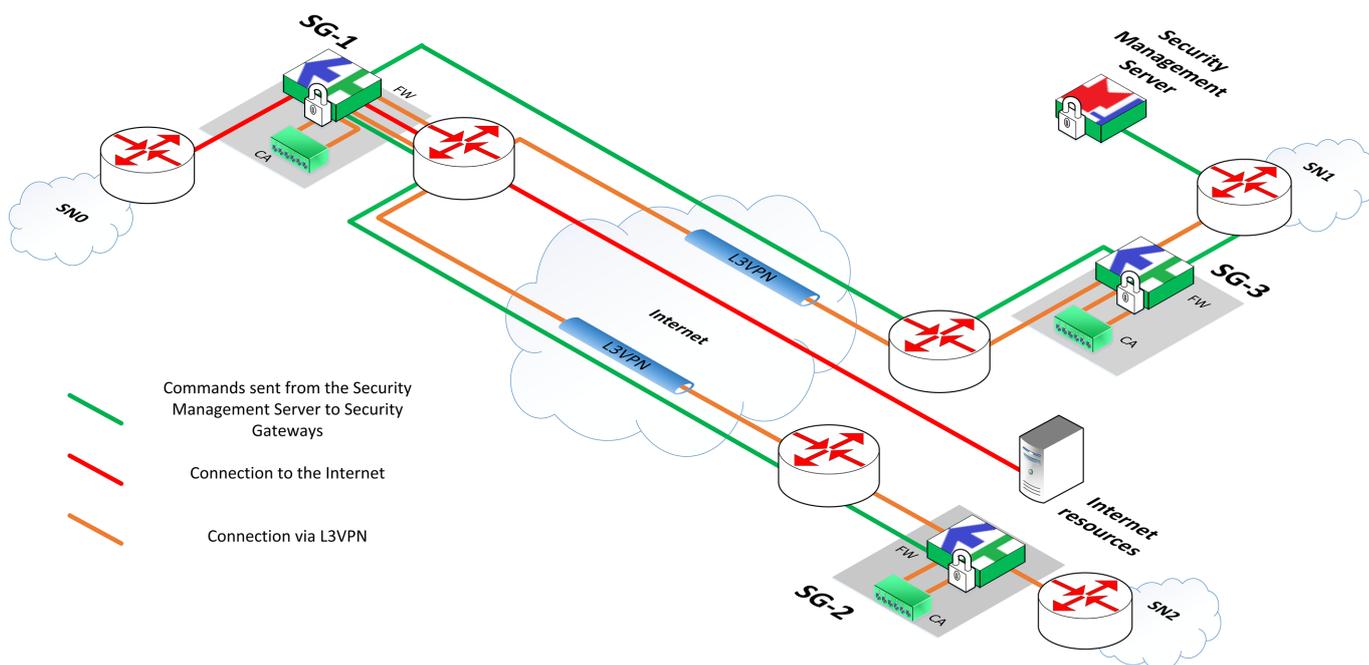
Cryptographic accelerator in star VPN topology

In star VPN topology, endpoint Security Gateways can encrypt data according to any scenario described above. A central Security Gateway can encrypt data according to the following scenarios:

- with pre-checking Firewall compliance and sending packets to a VPN channel from the cryptographic accelerator interface;
- without pre-checking Firewall compliance but with sending packets to a VPN channel from the Security Gateway interface;
- without pre-checking Firewall compliance but with sending packets to a VPN channel from the cryptographic accelerator interface.

Encryption without pre-checking Firewall compliance

The figure below illustrates the way of getting access from the secure network **SN2** to resources of the secure network **SN1**.



The central Security Gateway is **SG-1** that protects **SN0**.

SG-1 does not check transit packets for Firewall compliance.

The internal interface of **SG-2** receives IP packets from **SN2**, then checks them for Firewall compliance and sends them to the cryptographic accelerator for further encryption.

The cryptographic accelerator of **SG-2** encrypts and encapsulates packets, then sends them to **SG-2**.

SG-2 sends encrypted packets by its external interface to the central Security Gateway according to routing tables.

SG-1 receives encrypted packets by its external interface, then sends them to the cryptographic accelerator for further decryption.

The cryptographic accelerator of **SG-1** decrypts packets, then re-encrypts them and sends re-encrypted packets to **SG-1** for further sending to **SN3**.

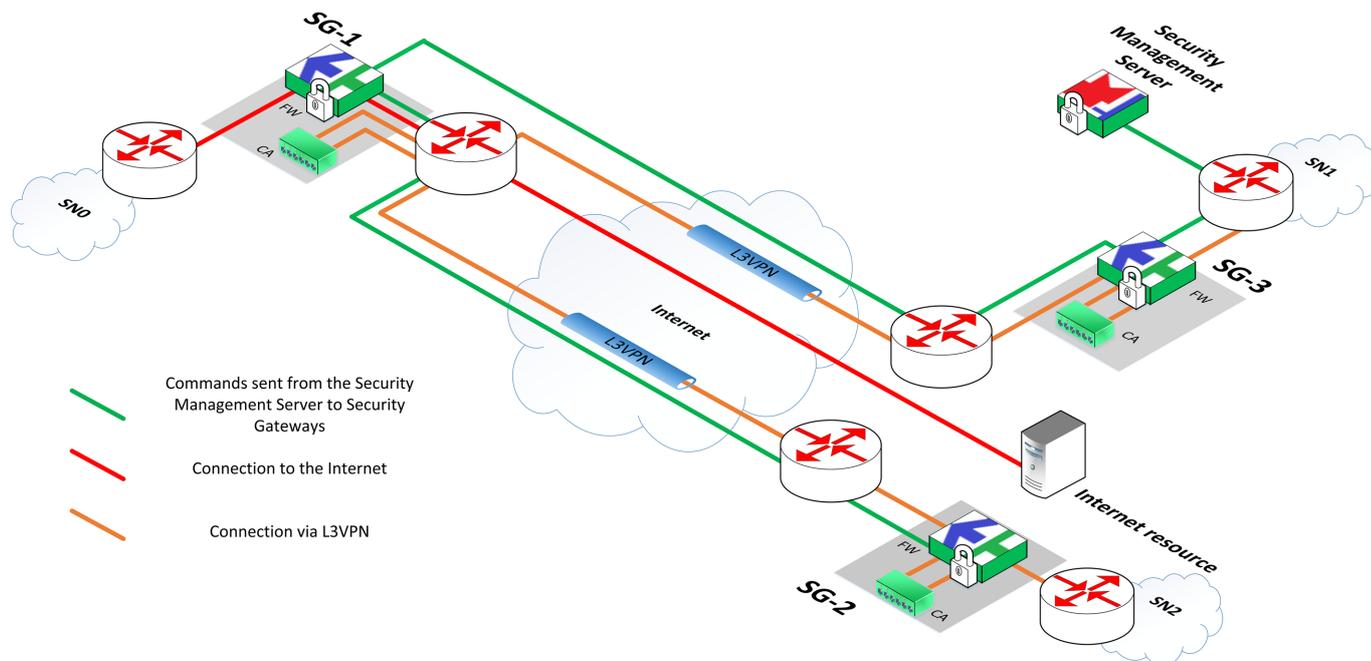
SG-1 encapsulates encrypted IP packets and sends them to **SG-3** by its external interface according to routing tables.

SG-3 receives encrypted packets by the external interface and sends them to the cryptographic accelerator.

The cryptographic accelerator decapsulates source IP packets, decrypts and sends them to **SG-3**.

SG-3 processes packets according to Firewall rules, then sends them to **SN1** by its own internal interface.

The following figure illustrates the other scenario, where the central Security Gateway uses external interfaces of the cryptographic accelerator to receive and send transit packets.



SG-2 receives IP packets by its internal interface.

SG-2 processes IP packets according to Firewall rules, then sends them to the cryptographic accelerator for further encryption.

The cryptographic accelerator encrypts IP packets, encapsulates them and sends to **SG-2**.

SG-2 sends encrypted packets by its external interface according to routing tables.

SG-1 receives IP packets by the external interface of the cryptographic accelerator.

The cryptographic accelerator decapsulates IP packets, decrypts and re-encrypts them, then encapsulates them.

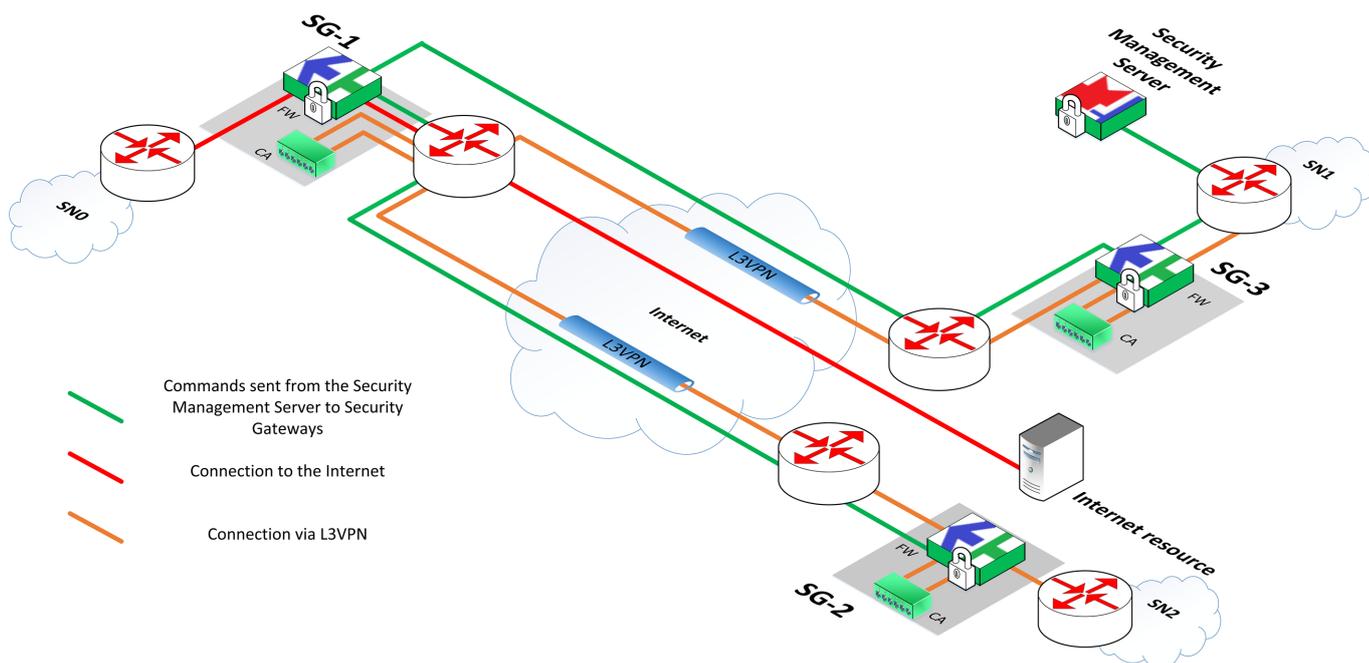
SG-1 sends encrypted packets by the external interface of the cryptographic accelerator to **SG-3** according to routing tables.

SG-3 receives encrypted packets by the external interface and redirects them to the cryptographic accelerator.

The cryptographic accelerator decapsulates source IP packets and sends them to **SN1** according to Firewall rules.

Encryption with pre-checking Firewall compliance

The figure below illustrates how **SG-1** checks transit packets for Firewall compliance. To send or receive transit packets, cryptographic accelerator interfaces are in use.



The internal interface of **SG-2** receives IP packets from the **SN2**.

SG-2 processes IP packets according to Firewall rules and sends them to the cryptographic accelerator for further encryption.

The cryptographic accelerator encrypts IP packets, encapsulates and sends them to **SG-2**.

SG-2 sends encrypted packets by its own external interface according to routing tables.

The cryptographic accelerator of **SG-1** receives encrypted packets, decapsulates source packets, decrypts and sends them to **SG-1**.

SG-1 checks packets for Firewall compliance and sends them to the cryptographic accelerator for further encryption.

The cryptographic accelerator of **SG-1** encrypts IP packets, encapsulates and sends them by its own external interface according to routing tables.

SG-3 receives IP packets by the internal interface, then sends them to the cryptographic accelerator.

The cryptographic accelerator decapsulates and decrypts source IP packets, then sends them to **SG-3**.

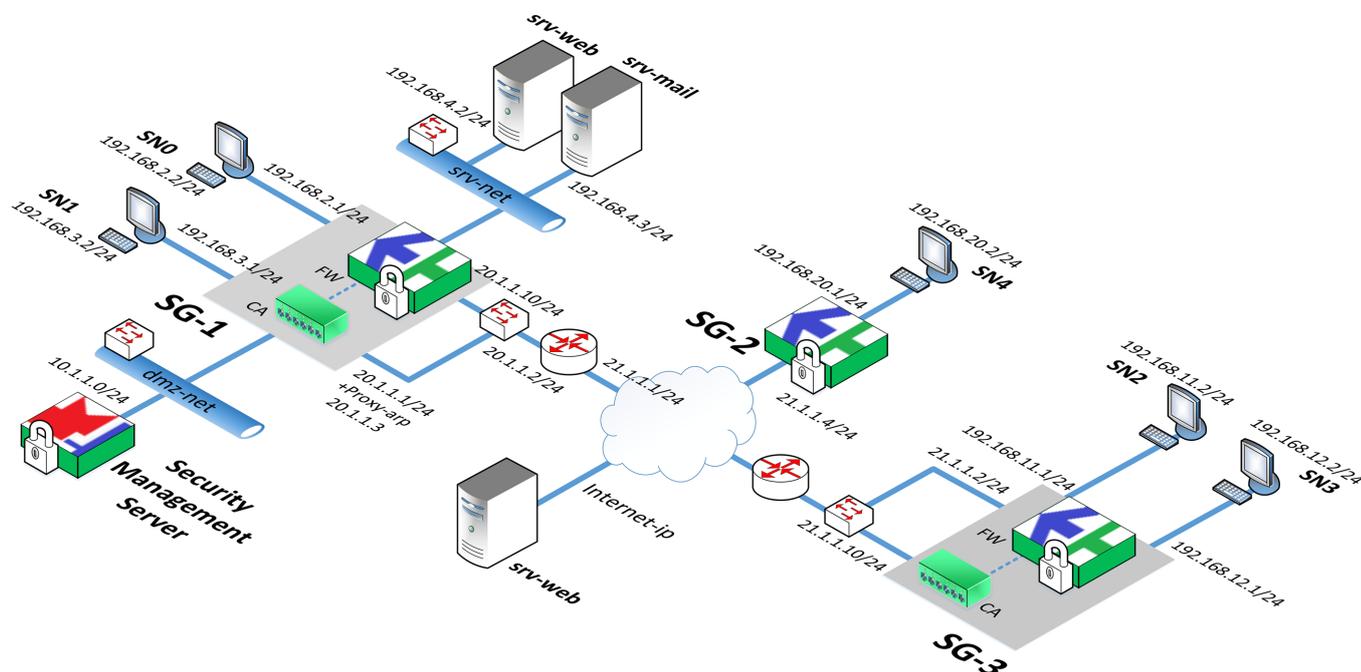
SG-3 processes IP packets according to Firewall rules and sends them to **SN1**.

Model scheme for using Security Gateways in VPN

The following figure illustrates a model scheme of using Security Gateways with the cryptographic accelerator in a corporate network of an enterprise.

Attention!

IP addresses specified in the model scheme are used as examples.



SG-1 with a cryptographic accelerator protects **SNO**, **SN1**, **dmz-net** and **srv-net** as Firewall. **SNO** is connected to the internal interface of **SG-1** and **SN1** is connected to the internal interface of its cryptographic accelerator.

SG-2 protects the subnet **SN4** but does not have a cryptographic accelerator integrated.

SG-3 protects **SN2** and **SN3**. **SN3** is connected to the internal interface of the cryptographic accelerator.

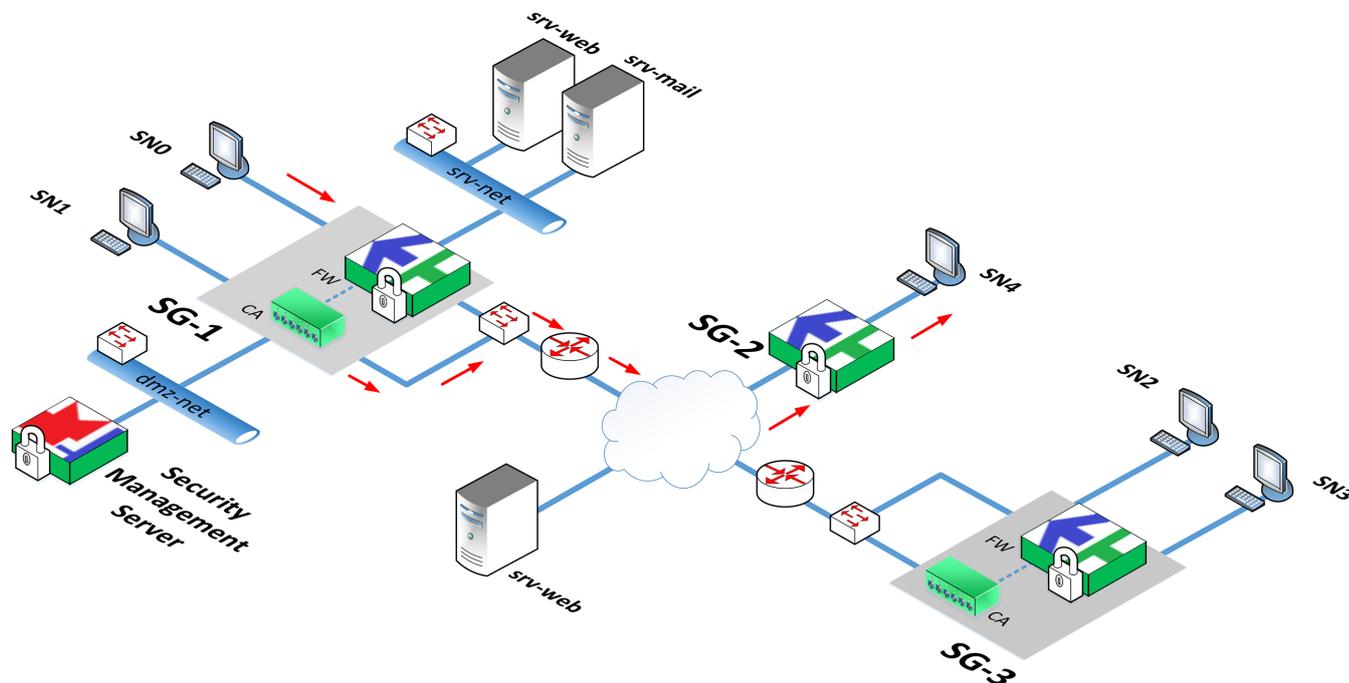
Scenarios of using cryptographic accelerators in a corporate network of an enterprise according to a previous scheme are described further. Scenarios with a star VPN topology are highlighted.

Examples of using the cryptographic accelerator in the model scheme

Access from a protected subnet to resources of other subnets

Scenario 1

The following figure illustrates a secure connection for **SN0** hosts (192.168.2.0/24) accessing **SN4** resources (192.168.20.0/24).



SG-1 receives packets from **SN0** hosts by its own internal interface (192.168.2.1/24), checks them for Firewall compliance, then encrypts them by the cryptographic accelerator and sends them by its own external interface (20.1.1.10/24).

Interfaces of **SG-1**:

Interface	Purpose	Address/Mask
ca0	External	20.1.1.10/24
te-0-0	Internal	192.168.2.1/24

Interfaces of **SG-2**:

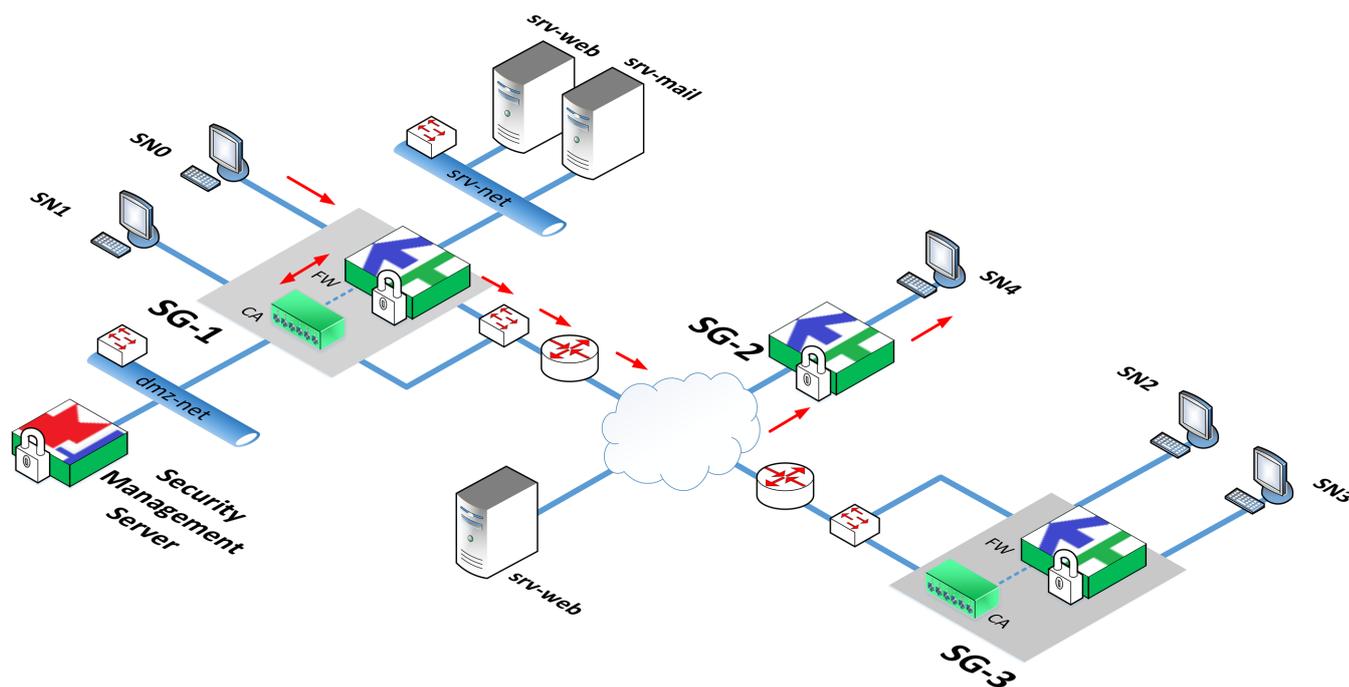
Interface	Purpose	Address/Mask
te-0-0	External	21.1.1.4/24
te-1-0	Internal	192.168.20.1/24

To pass traffic from **SN0** to **SN4**, you must install a Firewall rule on **SG-1** and **SG-2**. The rule must contain the following parameters:

Parameter	Value
Source	192.168.2.0/24
Destination	192.168.20.0/24
Service	Any
Application	Any
Action	Accept
Profile	None

Scenario 2

The following figure illustrates how packets are transferred from **SG-1** external interface (20.1.1.1/24) to the VPN channel. Interfaces of the cryptographic accelerator are not in use.



Interfaces of **SG-1**:

Interface	Purpose	Address/Mask
te-0-0	Internal	192.168.2.1/24
te-1-0	External	20.1.1.1/24

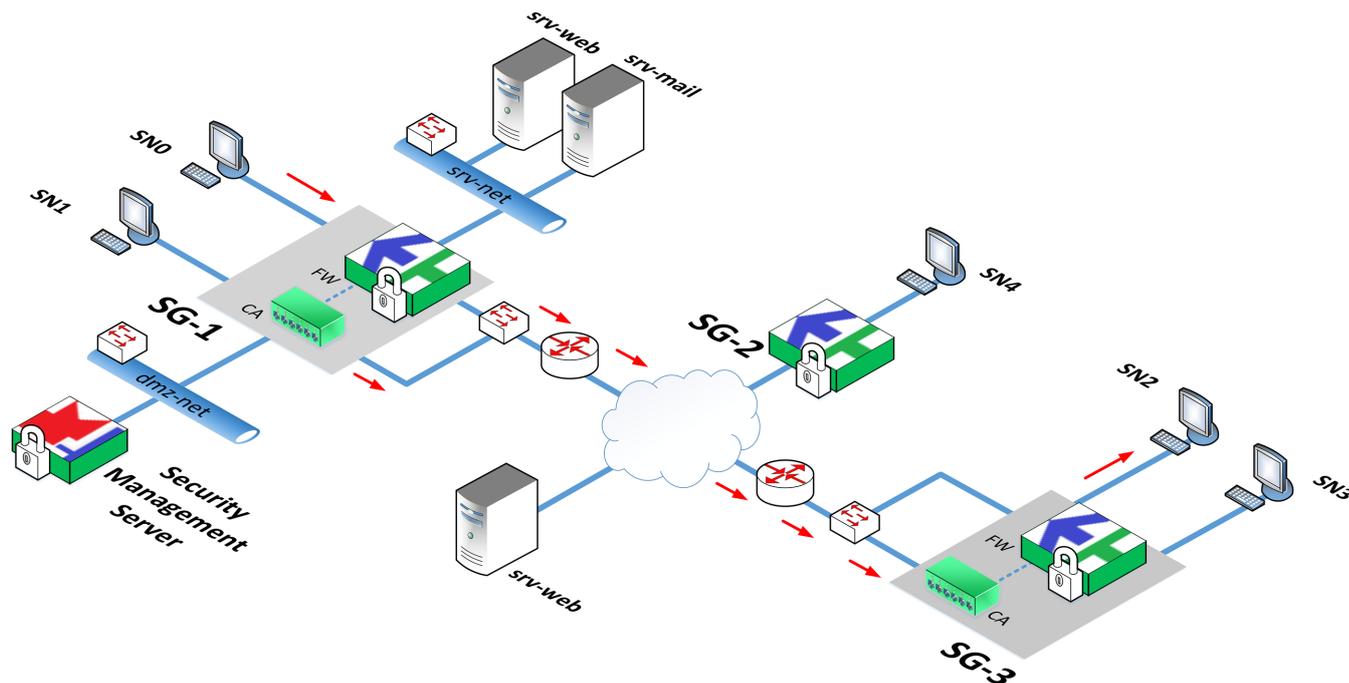
Interfaces of **SG-2** match Scenario 1.

To pass traffic from **SN0** to **SN4**, you must install a Firewall rule on **SG-1** and **SG-2**. The rule must contain the following parameters:

Parameter	Value
Source	192.168.2.0/24
Destination	192.168.20.0/24
Service	Any
Application	Any
Action	Accept
Profile	None

Scenario 3

The following figure illustrates the way of getting access from **SN0** to **SN2** (192.168.11.0/24).



Interfaces of **SG-1**:

Interface	Purpose	Address/Mask
ca0	External	20.1.1.10/24
ge-0-0	Internal	192.168.2.1/24

Interfaces of **SG-3**:

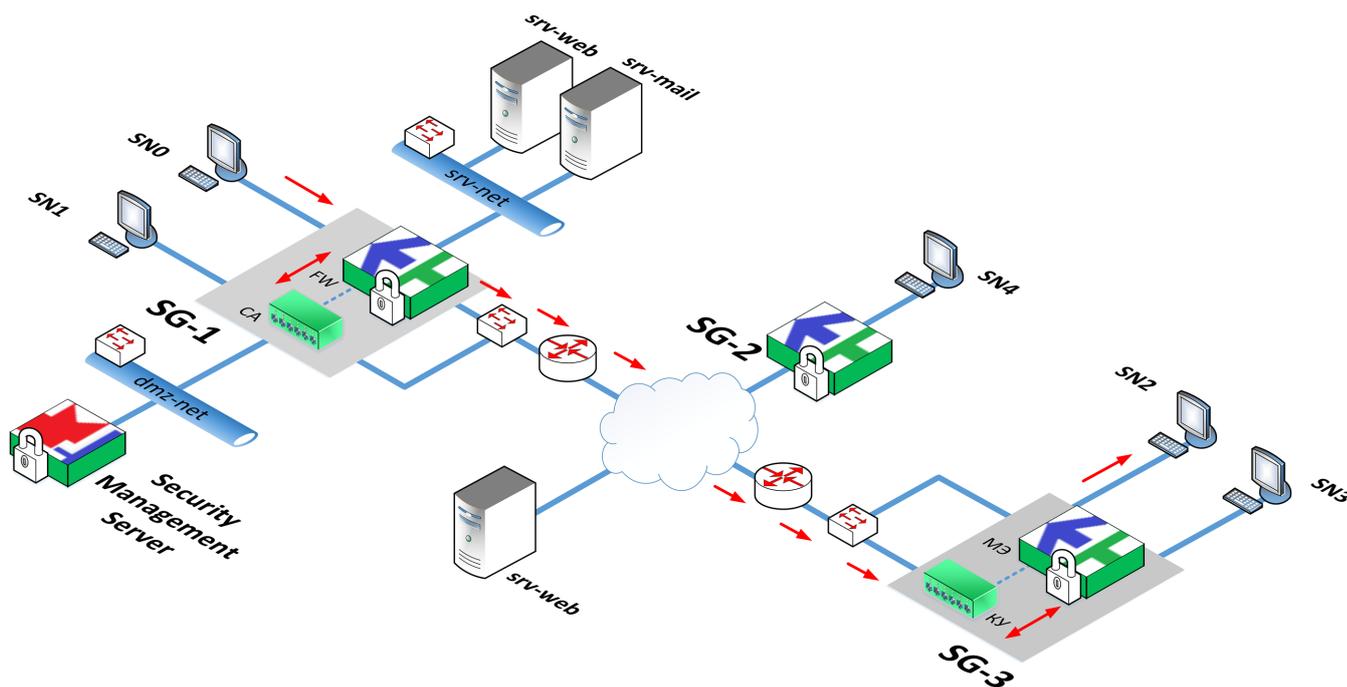
Interface	Purpose	Address/Mask
ca0	External	21.1.1.10/24
ge-0-0	Internal	192.168.11.1/24

To pass traffic from **SN0** to **SN2**, you must install a Firewall rule on **SG-1** and **SG-3**. The rule must contain the following parameters:

Parameter	Value
Source	192.168.2.0/24
Destination	192.168.11.0/24
Service	Any
Application	Any
Action	Accept
Profile	None

Scenario 4

The following figure illustrates the way of getting access from **SNO** to **SN2** (192.168.11.0/24). Interfaces of the cryptographic accelerator are not in use.



Interfaces of **SG-1**:

Interface	Purpose	Address/Mask
ge-0-0	Internal	192.168.2.1/24
ge-1-0	External	20.1.1.1/24

Interfaces of **SG-2**:

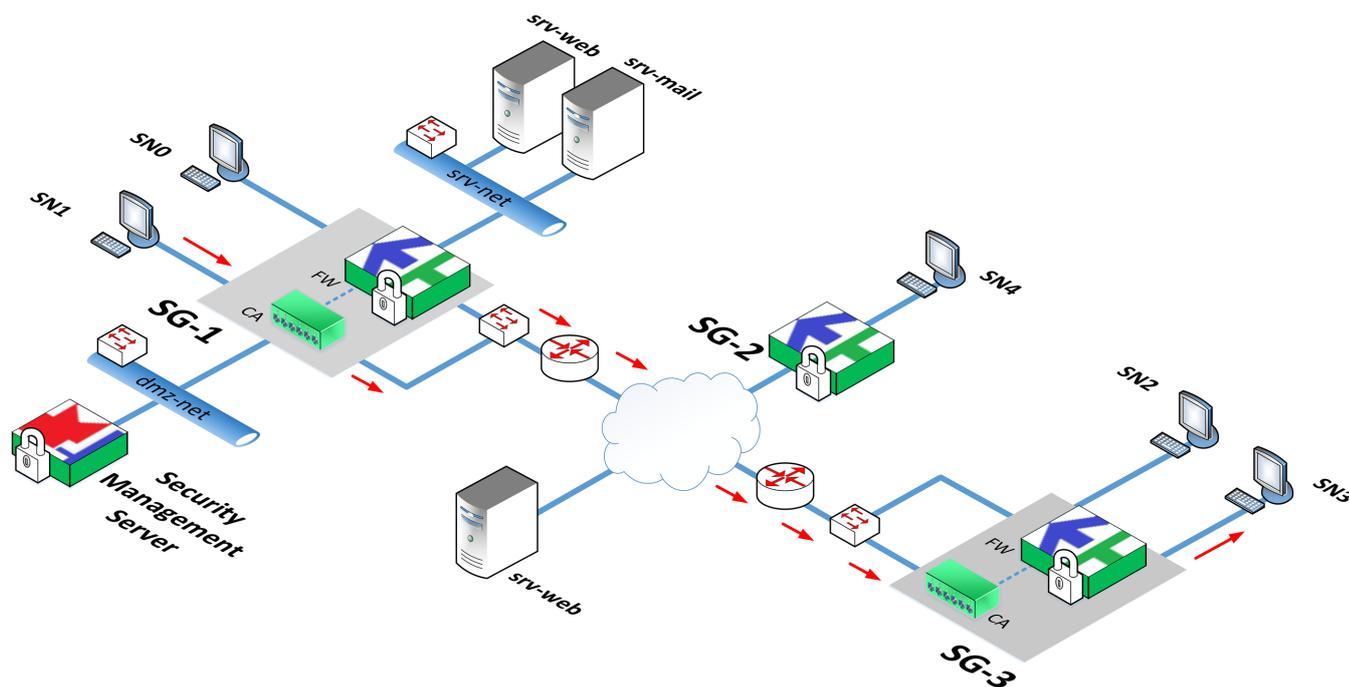
Interface	Purpose	Address/Mask
ge-0-0	Internal	192.168.11.1/24
ge-1-0	External	21.1.1.2/24

To pass traffic from **SNO** to **SN2**, you must install a Firewall rule on **SG-1** and **SG-3**. The rule must contain the following parameters:

Parameter	Value
Source	192.168.2.0/24
Destination	192.168.11.0/24
Service	Any
Application	Any
Action	Accept
Profile	None

Scenario 5

The following figure illustrates the way of getting access from **SN1** (192.168.3.0/24) to **SN3** (192.168.12.0/24) without pre-checking Firewall compliance on **SG-1** and **SG-3**.



Interfaces of **SG-1**:

Interface	Purpose	Address/Mask
ca0	External	20.1.1.10/24
ca1	Internal	192.168.3.1/24

Interfaces of **SG-3**:

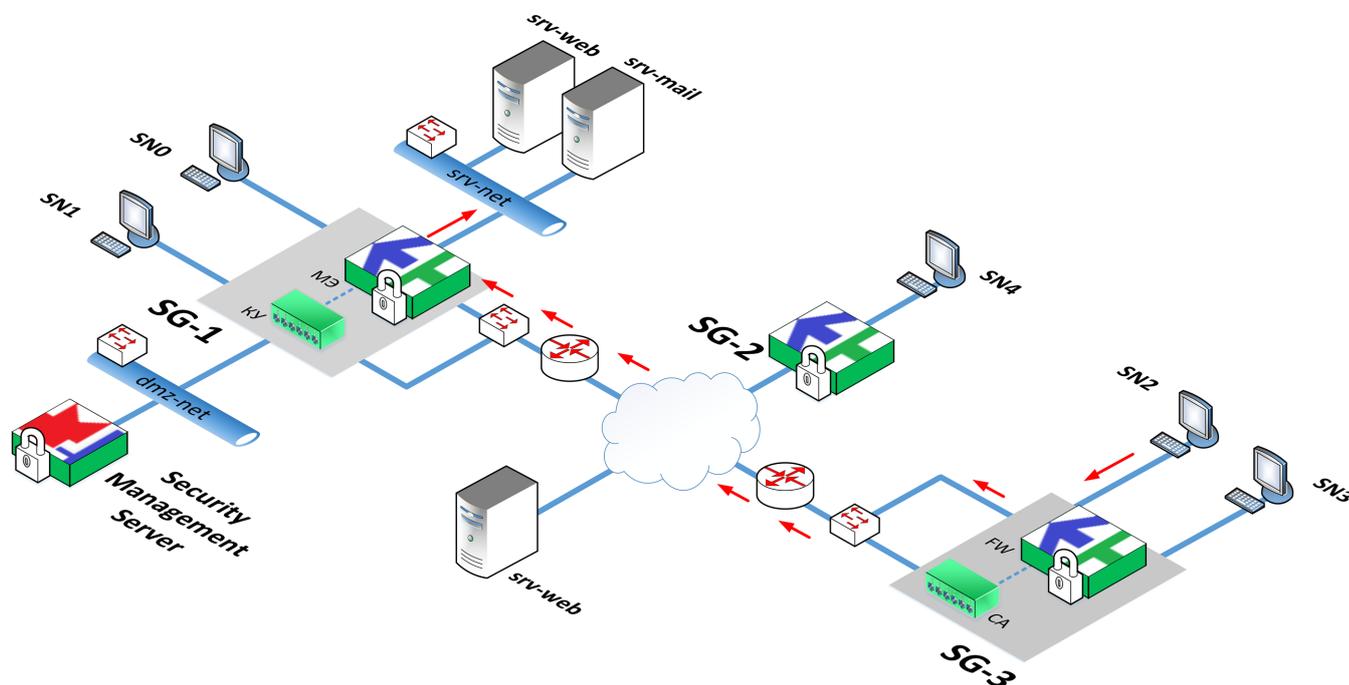
Interface	Purpose	Address/Mask
ca0	External	20.1.1.10/24
ca1	Internal	192.168.12.1/24

To transfer traffic from **SN1** to **SN3**, **SG-1** and **SG-3** do not need Firewall rules installed.

Access to corporate resources

Scenario 6

The following figure illustrates how a host (192.168.11.2/24) from **SN2** gets access to resources of **srv-net**: a web-server (192.168.4.2/24) and a mail-server (192.168.4.3/24). Corporate resources **srv-net** are protected by **SG-1**.



SN2 is connected to the internal interface of **SG-3** (192.168.11.1/24). **SG-3** checks packets received from the host of **SN2** according to Firewall rules, then sends them to the SG-1 by its external interface (21.1.1.2/24) without encryption.

SG-1 receives packets by the external interface (20.1.1.1/24), checks them for Firewall compliance and sends them to **srv-net** by its internal interface (192.168.4.1/24).

Attention!

If **SG-1** and **SG-3** use interfaces of the cryptographic accelerators, the purpose of the interface 21.1.1.2/24 sending packets from **SG-3** and the interface of **SG-1** that receives packets must be **None** (see below).

Interfaces of **SG-3**:

Interface	Purpose	Address/Mask
te-1-0	None	21.1.1.2/24
te-0-0	Internal	192.168.11.1/24

Interfaces of **SG-1**:

Interface	Purpose	Address/Mask
te-1-0	None	20.1.1.1/24
te-2-0	Internal	192.168.4.1/24

As the external interfaces of **SG-1** and **SG-3** have public IP addresses, you need to install NAT rules on **SG-1** and **SG-3** (for more information about NAT, see [2]).

The NAT rule for **SG-3**:

Original packet	
Source	192.168.11.2/24
Destination	20.1.1.1/24
Translated packet	

NAT type	Hide
Source	21.1.1.2/24
Destination	20.1.1.1/24

The NAT rule for **SG-1**:

Access to the web-server

Original packet	
Source	21.1.1.2/24
Destination	20.1.1.1/24
Translated packet	
NAT type	Destination
Source	21.1.1.2/24
Destination	192.168.4.2/24

Access to the mail-server

Original packet	
Source	21.1.1.2/24
Destination	20.1.1.1/24
Translated packet	
NAT type	Destination
Source	21.1.1.2/24
Destination	192.168.4.3/24

The Firewall rule for **SG-3** must contain the following parameters:

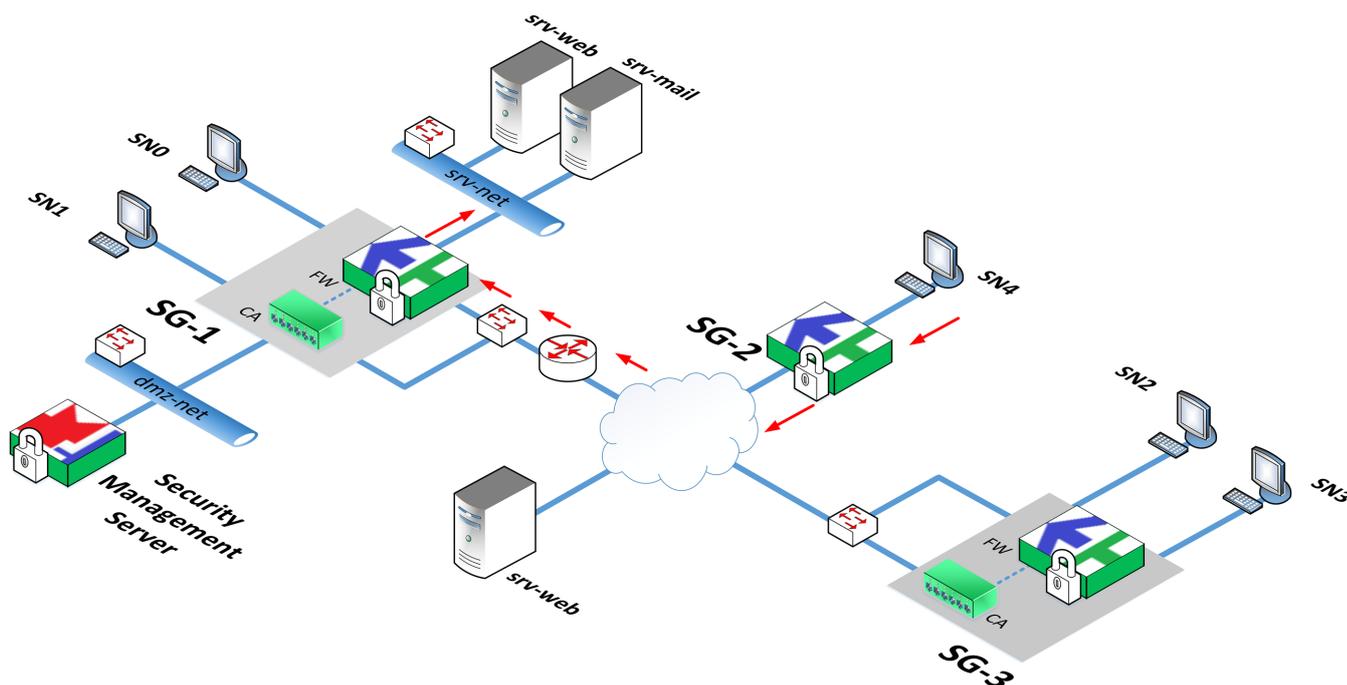
Parameter	Value
Source	192.168.11.2/24
Destination	20.1.1.0/24
Action	Accept

The Firewall rule for **SG-1** must contain the following parameters:

Parameter	Value
Source	21.1.1.0/24
Destination	20.1.1.0/24
Action	Accept

Scenario 7

The following figure illustrates how to get access from **SN4** to corporate resources of the host **192.168.20.2/24** protected by **SG-2** without the cryptographic accelerator.



SG-2 receives packets from the host of **SN4** by the internal interface (192.168.20.1/24), checks them for Firewall compliance, then sends them without encryption to **SG-1** by its external interface (21.1.1.4/24).

Interface	Purpose	Address/Mask
te-0-0	External	21.1.1.4/24
te-1-0	Internal	192.168.20.1/24

Interfaces of **SG-1** match Scenario 6.

The NAT rule for **SG-2**:

Original packet	
Source	192.168.20.2/24
Destination	20.1.1.1/24
Translated packet	
NAT type	Hide
Source	21.1.1.4/24
Destination	20.1.1.1/24

NAT rules for **SG-1** match Scenario 6.

The Firewall rule for **SG-2** must contain the following parameters:

Parameter	Value
Source	192.168.20.2/24
Destination	20.1.1.0/24
Action	Accept

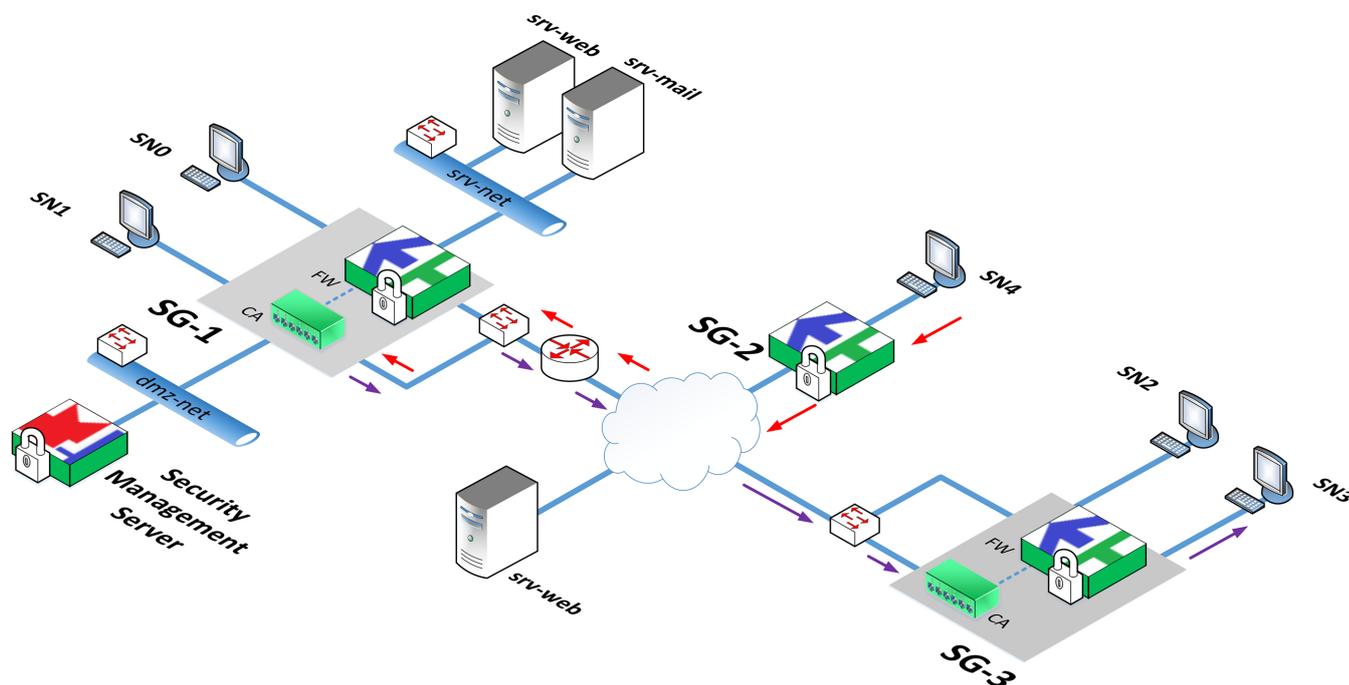
The NAT rule for **SG-1** matches Scenario 6.

Configuration for star VPN topology

SG-1 is the central Security Gateway in all the following scenarios.

Scenario 8

The following figure illustrates the way of getting access from **SN4** to **SN3**.



SG-2 receives packets from **SN4** by its own internal interface, then checks them for Firewall compliance, encrypts and sends them to **SG-1** by its own external interface.

The cryptographic accelerator of **SG-1** receives encrypted packets by its own external interface, decrypts them, then re-encrypts and sends them to **SG-3** by the external interface.

The cryptographic accelerator of **SG-3** receives encrypted packets by the external interface, then decrypts and sends them to **SN3** by the internal interface.

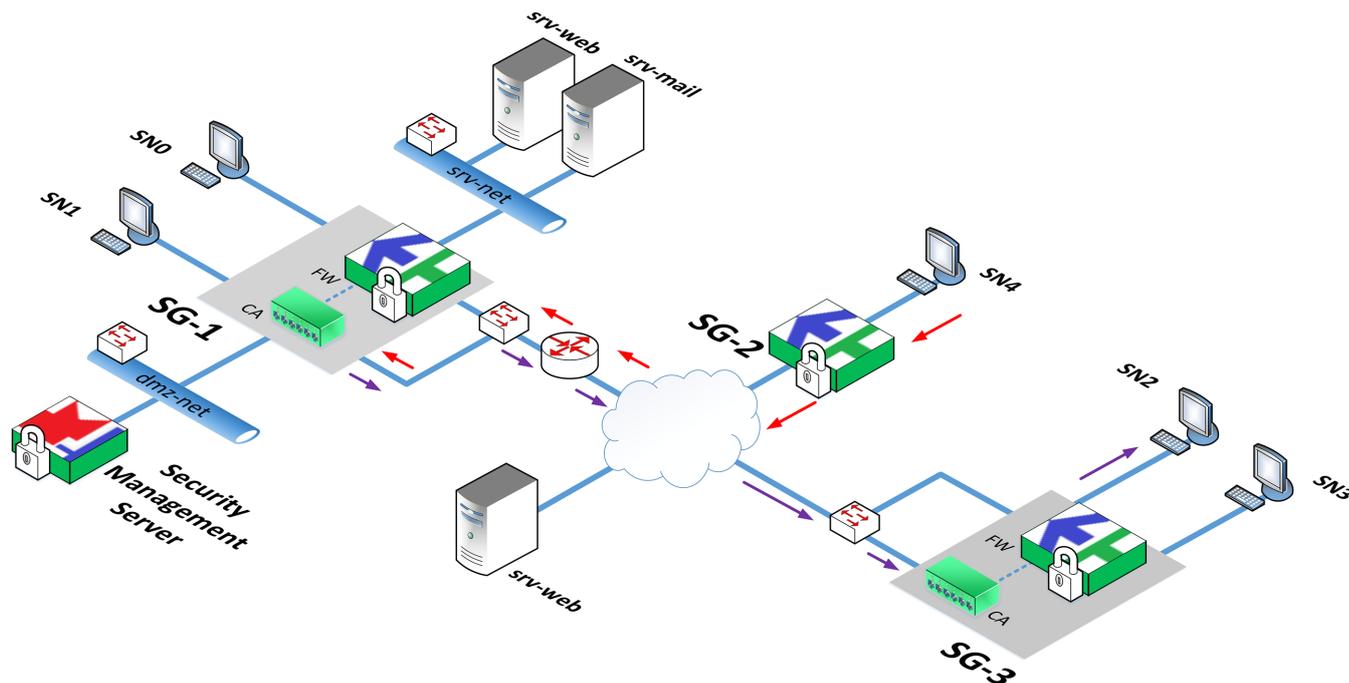
To implement this scenario, you need to configure interfaces of the Security Gateways and create a Firewall rule accepting traffic from **SN4** hosts to **SN3** hosts for **SG-2**.

Note.

Packet routes from **SG-2** to **SG-3** will be created automatically if you select star VPN.

Scenario 9

The following figure illustrates the way of getting access from **SN4** to **SN2**.



SG-2 receives packets from **SN4** by its own internal interface, then checks them for Firewall compliance, encrypts and sends them to **SG-1** by its own external interface.

The cryptographic accelerator of **SG-1** receives encrypted packets by its own external interface, decrypts them, then re-encrypts and sends them to **SG-3** by the external interface.

SG-3 receives encrypted packets by the external interface of its own cryptographic accelerator that previously decrypted them, checks them for Firewall compliance, then sends them to **SN2** by the internal interface.

SG-3 checks packets decrypted by its cryptographic accelerator for Firewall compliance.

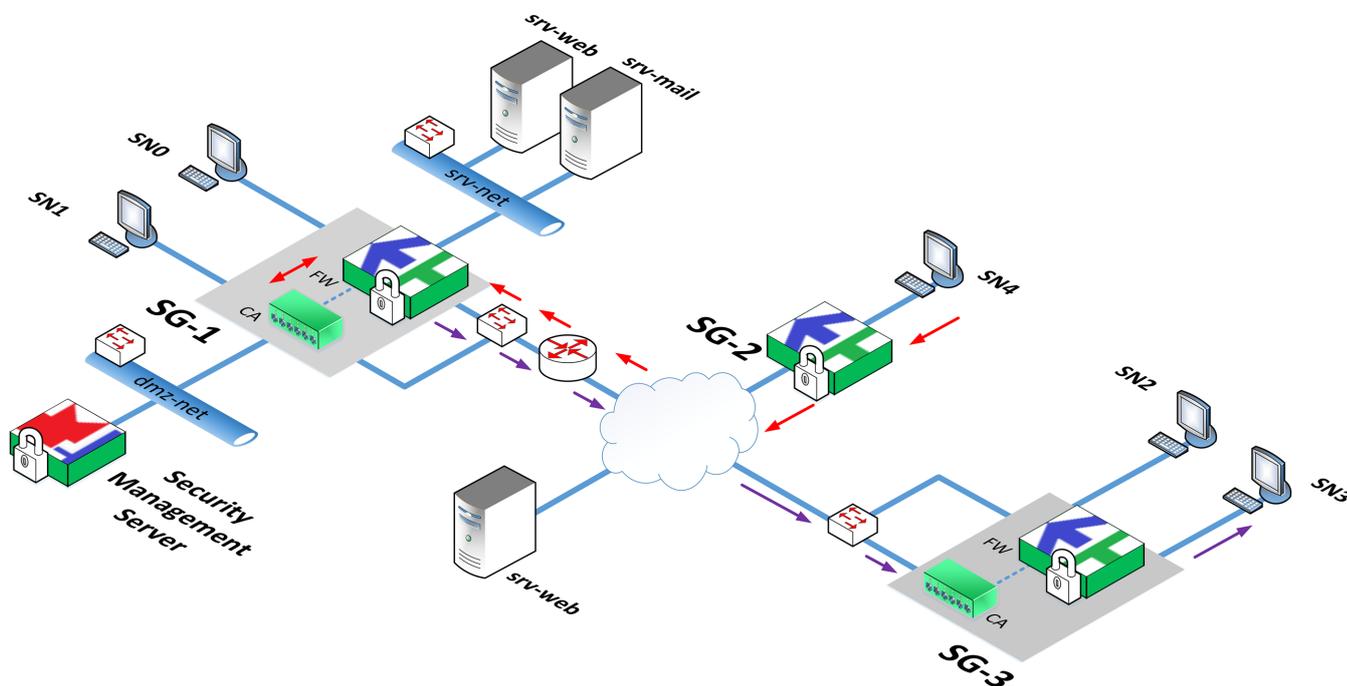
To send packets from **SN4** to **SN2**, **SG-2** and **SG-3** must have the respective Firewall rule installed and its own interface must be set as internal.

Encryption on the central Security Gateway without pre-checking Firewall compliance

The following scenarios describe the way the central Security gateway encrypts packets without pre-checking Firewall compliance. In those scenarios, interfaces of **SG-1** cryptographic accelerator are not in use.

Scenario 10

The following figure illustrates the way of getting access from **SN4** to **SN3**.



SG-2 receives packets from **SN4** by its own internal interface, then checks them for Firewall compliance, encrypts and sends them to **SG-1** by its own external interface.

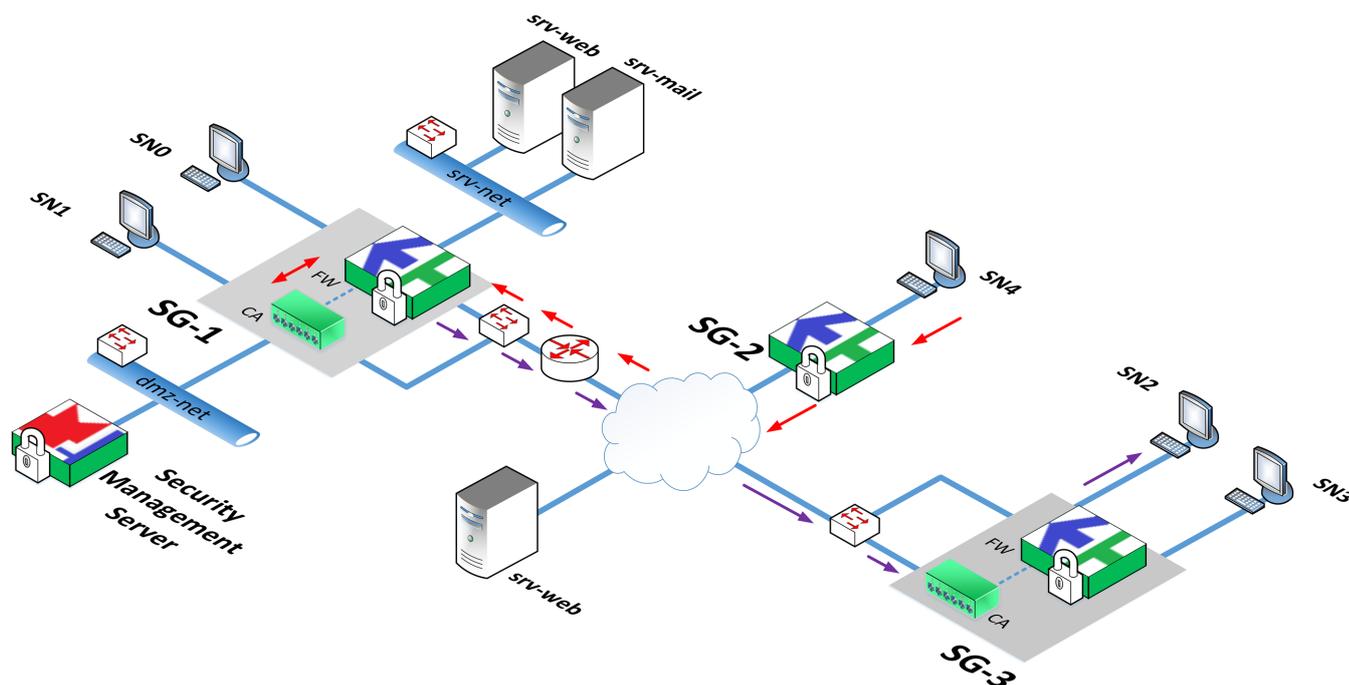
SG-1 receives encrypted packets by its own external interface, decrypts them by the cryptographic accelerator, then re-encrypts and sends the encrypted packets to **SG-3** by its own external interface.

The cryptographic accelerator of **SG-3** receives encrypted packets by the external interface, then decrypts and sends them to **SN3** by the internal interface.

To implement this scenario, you need to create a Firewall rule accepting traffic from **SN4** hosts to **SN3** hosts for **SG-2**.

Scenario 11

The following figure illustrates the way of getting access from **SN4** to **SN2**, where **SN2** is connected to the internal interface of **SG-3**.



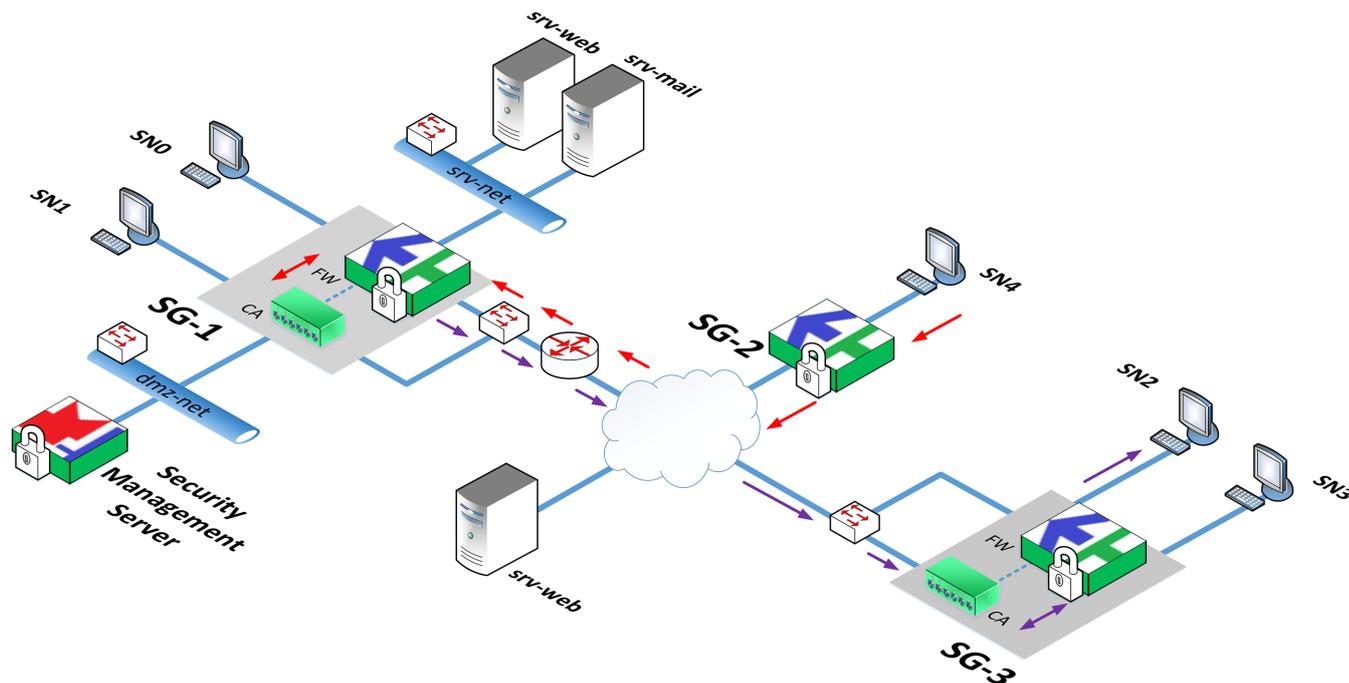
The **SG-2** receives packets from **SN4** by its own internal interface, then checks them for Firewall compliance, encrypts and sends them to the **SG-1** by its own external interface.

The **SG-1** receives encrypted packets by its own external interface, decrypts them by the cryptographic accelerator, then re-encrypts and sends encrypted packets to the **SG-3** by its own external interface.

The **SG-3** receives encrypted packets by the external interface of the cryptographic accelerator that afterwards decrypts them, checks them for Firewall compliance and sends them to **SN2** by its own internal interface.

Scenario 12

The following figure illustrates the way of getting access from **SN4** to **SN2**.



The **SG-2** receives packets from **SN4** by its own internal interface, then checks them for Firewall compliance, encrypts and sends them to the **SG-1** by its own external interface.

The **SG-1** receives encrypted packets by its own external interface, decrypts them by the cryptographic accelerator, then re-encrypts and sends encrypted packets to the **SG-3** by its own external interface.

The **SG-3** receives encrypted packets by its own external interface, decrypts them by the cryptographic accelerator, checks them for Firewall compliance and sends them to **SN2** by its own internal interface.

For the implementation of the scenarios 11 and 12, you must install the Firewall rule accepting traffic from **SN4** to **SN2** on **SG-2** and **SG-3**.

Chapter 4

L2VPN deployment

Overview

In Continent, L2VPN is a virtual switch connecting network interfaces of Security Gateways to a distributed network bridge. Network interfaces of Security Gateways operate as switch ports of a network bridge.

If you add ports of different Security Gateways to a virtual switch, VPN tunnels between them are created automatically. These tunnels ensure secure transfer of Ethernet frames.

A virtual switch port passes traffic for STP, RSTP, MSTP, MVRP, LACP and LLDP.

Using Security Gateway ports, you can create a bridge which in its turn can be included in virtual switch.

A virtual switch supports port security options:

- limit MAC addresses count in the switching table;
- create a static MAC address in the switching table of a virtual switch (binding a MAC address to a specific virtual switch port);
- prohibit unicast packet transfer for unknown MAC addresses;
- configure a reaction to a security violation.

A virtual switch can operate in the following modes:

Mode	Description
Default	The split horizon method is used to prevent switching loops and broadcast storms. Cryptographic accelerator ports pass BPDU of STP, RSTP, MSTP
Transparent	Virtual switch ports pass standard BPDU (STP, RSTP, MSTP, MVRP, LACP, LLDP protocols). This mode does not affect passing standard BPDU (such as PAgP)
Spanning Tree Protocol (STP)	STP is used to prevent switching loops. Connections not used in single-hop interconnectivity are blocked automatically
Pseudo wire	Emulates standard services over networks with packet switching. Transparently transfers ATM, Frame relay, Ethernet, low-speed TDM or SDH/SONET over networks with MPLS, IP (IPv4 or IPv6) or L2TPv3 packet switching. Only for a virtual switch with two ports. Switching table is not in use. Transparent mode is enabled, port security is not in use

L2VPN can handle the following security violations:

- the detection of known MAC address duplication beyond another switch port;
- an access attempt to a switch port (a MAC address is not in the static address list or dynamic table is overflowed).

Reactions to events:

- no reaction;
- port down;
- log events to syslog and network security log;
- log and port down.

Commutation table in a virtual switch can be formed in one of three ways:

- dynamic learning — the table containing MAC addresses is filled automatically (dynamic addresses);
- dynamic learning is disabled — host MAC addresses are assigned to the ports of a virtual switch manually by the administrator (static addresses);
- Sticky learning mode — dynamic MAC addresses are assigned to a virtual switch as static ones.

Attention!

When a virtual switch is switched from dynamic to sticky learning, MAC addresses remain **Dynamic** type. To change the type of MAC address to Static, it is recommended to turn off the virtual switch (that operated in the dynamic learning mode), install policy on the respective Security Gateways, turn on the virtual switch and install policy on the Security Gateway again.

Configure L2VPN

To configure L2VPN, take the following steps:

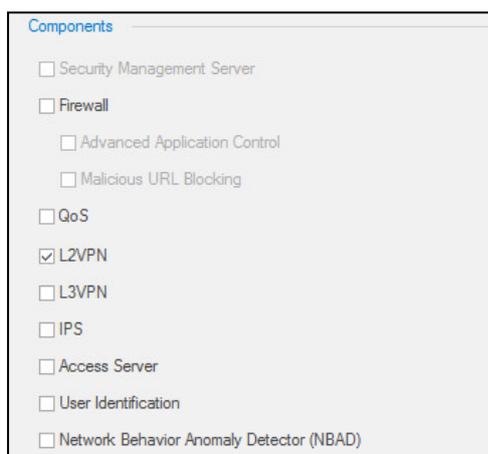
1. On the Security Gateways, configure network interfaces operating in L2 mode.
2. Create a virtual switch (see p. 42).
3. Configure a virtual switch (see p. 45).

Configure network interfaces

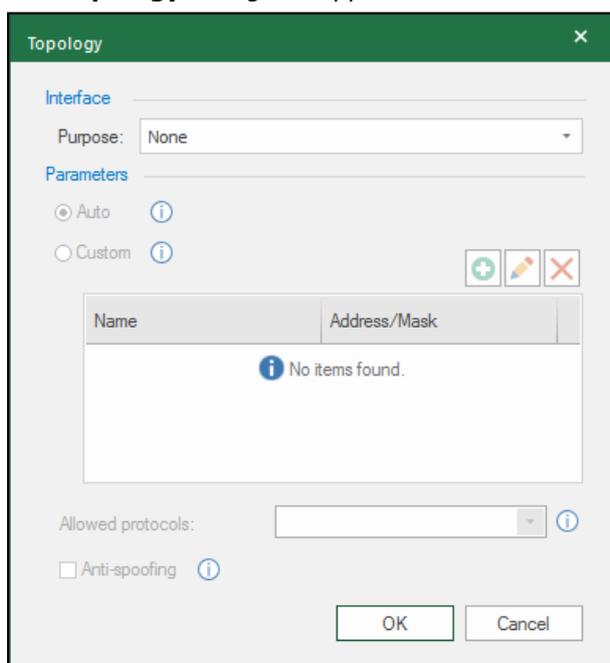
You need to configure each Security Gateway which ports must be a part of the virtual switch.

To configure interfaces:

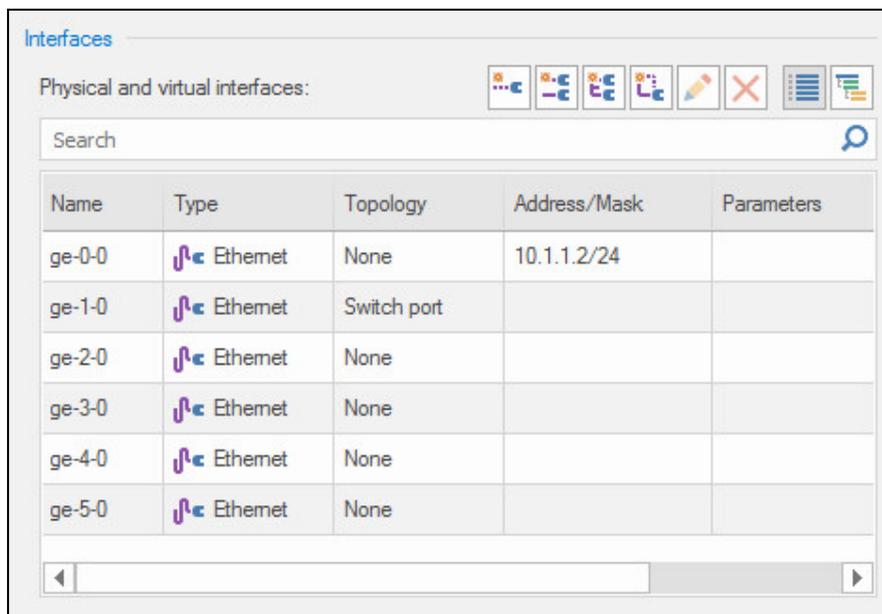
1. In the Configuration Manager, go to **Structure**.
The list of registered Security Gateways appears in the display area.
2. Right-click the required Security Gateway and click **Properties**.
The **Security Gateway** dialog box appears.
3. Enable L2VPN by selecting the respective check box as in the figure below.



4. On the left, click **Interfaces**.
The list of Security Gateway interfaces appears.
5. Select the interface required for L2VPN and double-click the **Topology** cell.
The **Topology** dialog box appears.



6. In the **Purpose** field, select **Switch port** and click **OK**.
The **Topology** dialog box is closed and **Switch port** appears in the **Topology** column.



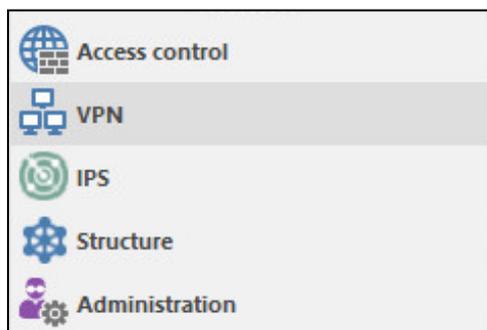
- If you want to use other interfaces of the Security Gateway as switch ports, repeat steps **5-6**. After configuring all the interfaces, click **OK**.
- Go to the list of Security Gateways, select the next Security Gateway and repeat steps **2-7**. After configuring all interfaces of all the Security Gateways included in L2VPN, create a virtual switch (see p. **42**).

Virtual switches

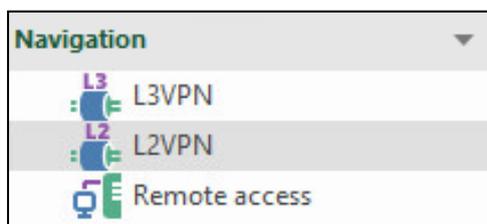
View the list of virtual switches

To go to the list of virtual switches:

- In the Configuration Manager, go to **VPN**.



- In the **Navigation** group, select **L2VPN**.



The list of the created virtual switches appears in the display area.

Note.

If there are no created virtual switches, the list is empty.

In the figure below, you can see the list consisting of two virtual switches **VS-1** and **VS-2**.

Security gateway	Port	Static MAC Address	Learning	Table size	Reaction on violation	Description
VS-1						
SG-1	ge-4-0		On	-	None	
SG-2	ge-4-0		On	-	None	
VS-2						
SG-1	ge-5-0		On	-	None	
SG-2	ge-5-0		On	-	None	

For each virtual switch, there is a list of ports indicating the Security Gateway to which the port belongs. You can find the following information about each port:

- port name;
- list of static MAC addresses of devices in the protected network;
- dynamic learning mode (on/off);
- switching table size;
- reaction to security violations;
- description (additional information about a port).

Create a new virtual switch

To create a new virtual switch:

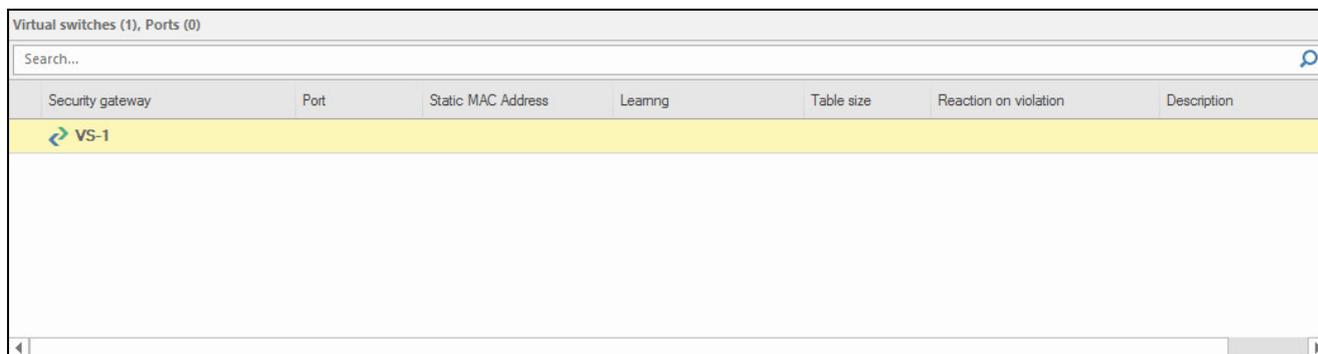
1. Go to the list of virtual switches (see p. 42) and click **Virtual switch** on the toolbar.



The **Virtual switch** dialog box appears.

 A dialog box titled "Virtual switch" with a close button (X). It contains a "Name:" field with "VS-1" entered, a "Description:" text area, and an "Options" group box. The "Options" group box has four radio buttons: "Default" (selected), "Transparent", "STP", and "Pseudo Wire". Each radio button has an information icon (i) to its right. At the bottom are "OK" and "Cancel" buttons.

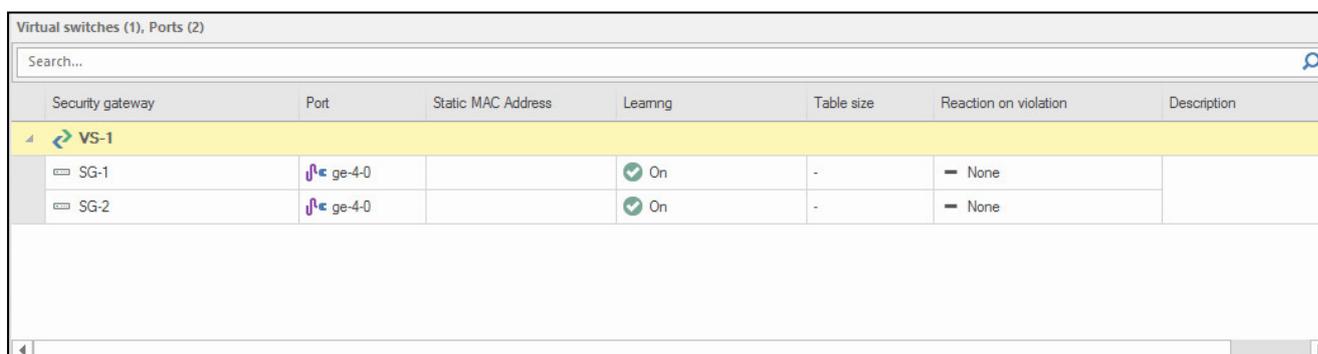
2. Enter the required name description.
You can use English uppercase and lowercase characters, base 10 digits and special characters `!@#\$%^()-=_+[]';,`.
3. If necessary, select the options of virtual switch operation: **Transparent**, **STP**, **Pseudo Wire** in the **Options** group box.
4. Click **OK**.
The created virtual switch appears in the list.



- Select the required virtual switch and click **Add port** on the toolbar. The **Port** dialog box appears.



- In the **Security Gateway** drop-down list, select the required Security Gateway. In the **Interface** drop-down list, the Security Gateway interface name with the **Switch port** topology appears. If there are several interfaces, select the required one from the drop-down list.
- Click **OK**. The switch port will be added to the virtual switch.



By default, the added port has the following parameters:

- **Static MAC Address** — empty;
- **Learning** — On;
- **Table size** — Not limited (value — '-');
- **Reaction to violations** — None.

- Specify the parameters of the port by selecting it and entering the required value.

Note.

You can specify the port parameters after you add other ports to the virtual switch.

When entering static MAC addresses, use the following format — **00:00:00:00:00:00**. When specifying several MAC addresses, separate them by pressing **<Enter>**.

Attention!

- We do not recommend saving the default table size. Specify a value that matches with the number of hosts on the switched network.
- In **STP** mode, MAC addresses of tunnel interfaces used to exchange STP packets are taken into consideration when counting the total number of MAC addresses that is limited by the switching table size.

- To add another port, repeat steps **6-9**.
- After adding all the required ports, save the changes.

Delete a virtual switch

To delete a virtual switch:

1. In the Configuration Manager, go to **VPN** and select **L2VPN**.
The list of virtual switches appears.
2. Select a required virtual switch and click **Delete** on the toolbar.
The dialog box prompting you to confirm the action appears.
3. Click **Yes**.
The selected virtual switch will be deleted.

Configure parameters of a virtual switch

Configuring the parameters of a virtual switch includes the following actions:

- edit general parameters (name, description, options);
- add ports to the virtual switch or remove them;
- configure parameters of ports.

To edit general parameters of a virtual switch:

1. Select the required virtual port and click **Properties** on the toolbar.
The **Virtual switch** dialog box appears (see p. 43).
2. Make the required changes and click **OK**.
3. To save the changes, click **Save** on the toolbar.

To add a port:

1. Select the required virtual port and click **Add port** on the toolbar.
The **Port** dialog box appears (see p. 43).
2. Take steps 6-8 (see p. 43).
3. To save the changes, click **Save** on the toolbar.

To remove a port:

1. Right-click the required port and click **Remove**.
You receive a message about the port removal.
2. Click **Yes**.
The port is removed from the virtual switch.
3. To save the changes, click **Save** on the toolbar.

To configure port parameters:

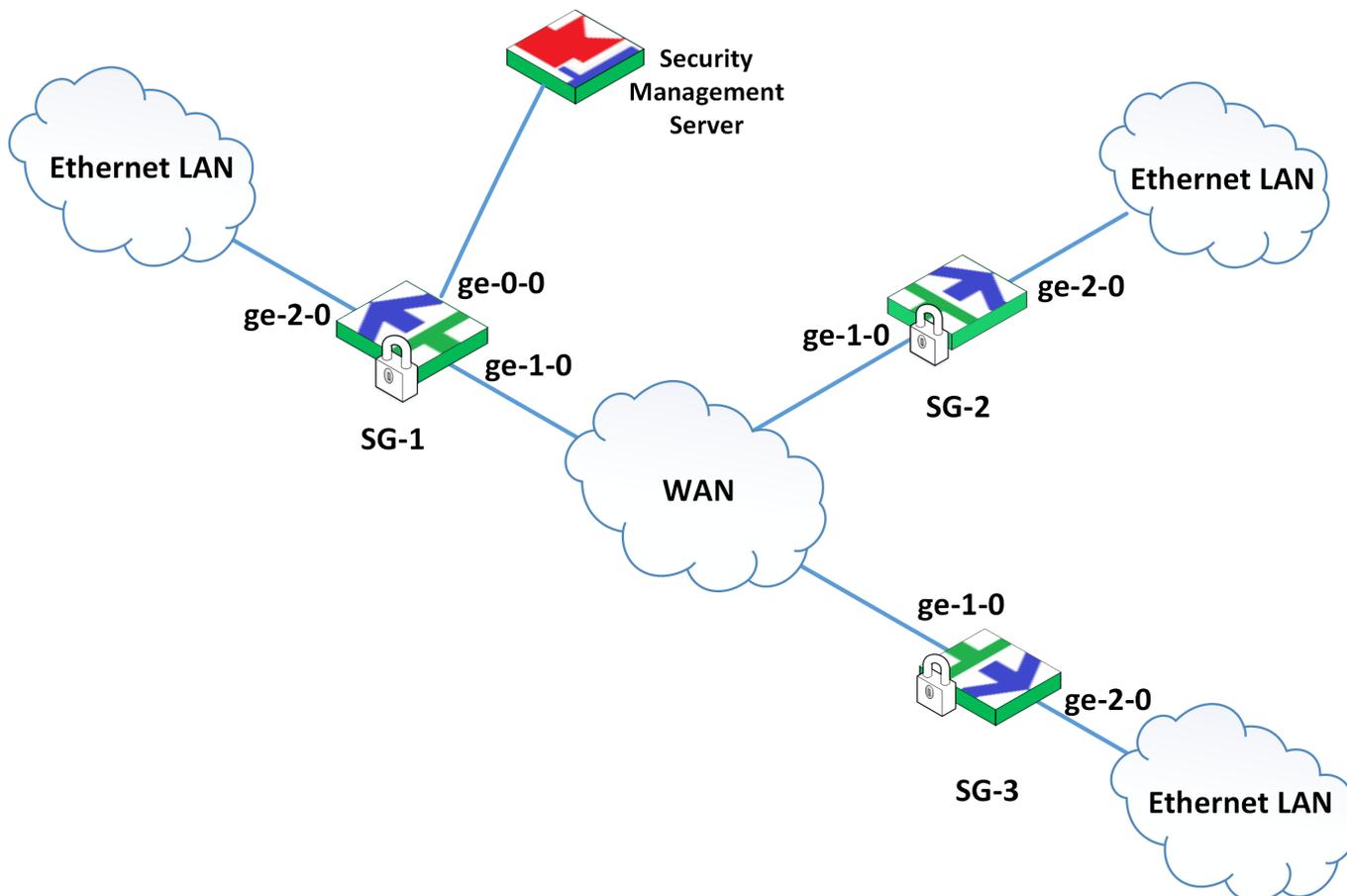
1. Select the required parameter and specify a value.
2. To save the changes, click **Save** on the toolbar.

Model scheme of using L2VPN

This section provides examples of using L2VPN. Security Gateways are connected to the Ethernet LAN using the internal interface **ge-2-0**. The external interfaces **ge-1-0** are used to connect to the WAN.

Model scheme 1

The figure below displays connected Ethernet LAN local networks. This requires switching between tagged and non-tagged frames and transparently allowing service traffic (standard PDU).



To configure L2VPN and meet the requirements, follow the common configuration steps (see p. 40).

When configuring network interfaces, set the ge-2-0 interfaces as switch ports for **SG-1**, **SG-2**, **SG-3**.

When creating a virtual switch, select **Transparent** in the advanced parameters and add the ge-2-0 interfaces of each Security Gateway to the virtual switch.

As a result of the configuration, user and service traffic passes through local networks. User traffic contains tagged (VLAN id 1 – 4096) and non-tagged frames. Service traffic contains standard PDU (STP, RSTP, MSTP, LLDP, LACP).

Model scheme 2

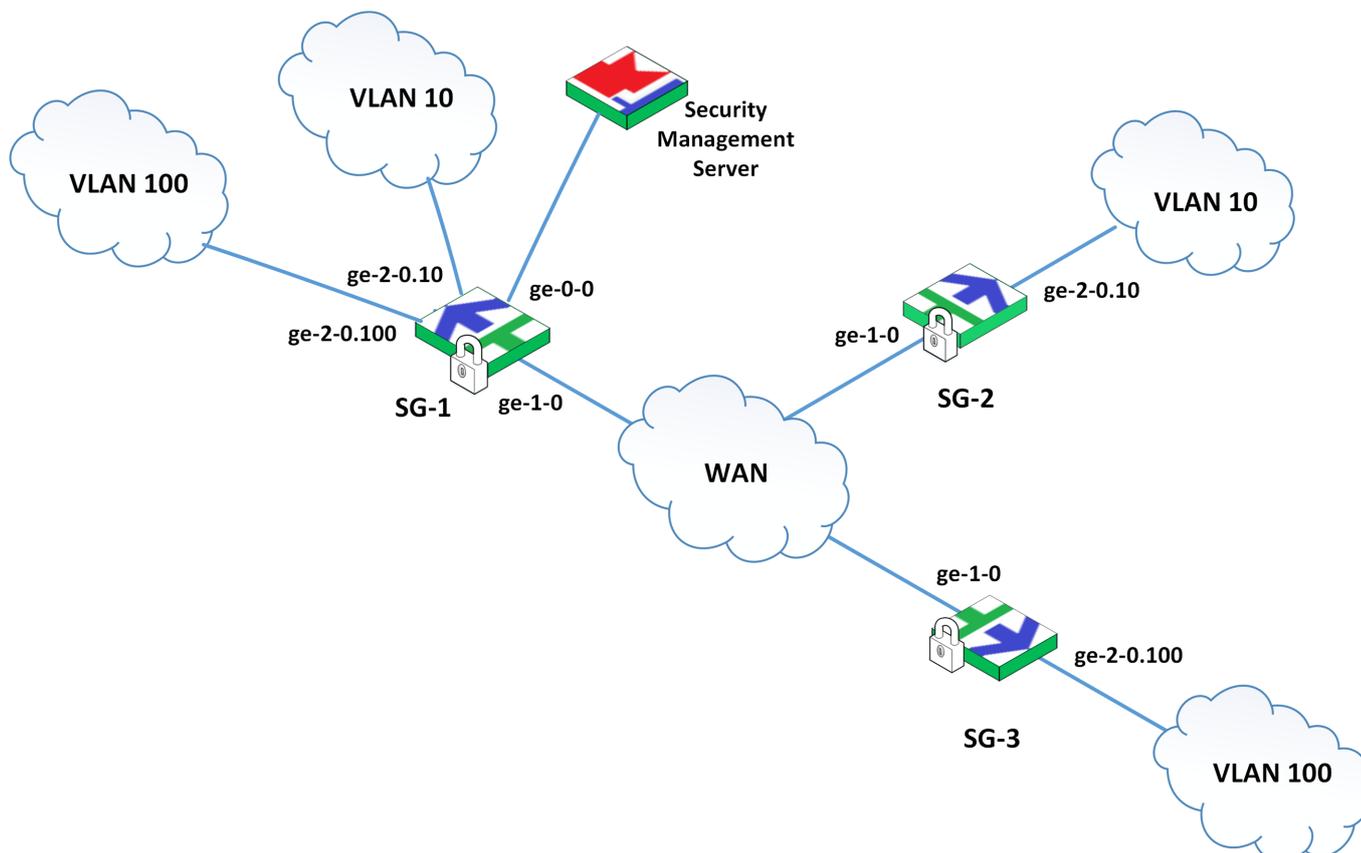
This scheme is similar to scheme 1 but service traffic (standard PDU) is not allowed.

Unlike scheme 1, select **By default** value while creating the virtual switch.

As a result of the configuration, the user and service traffic passes through local networks. User traffic contains tagged (VLAN id 1 – 4096) and non-tagged frames. Service traffic that arrives from the protected network and contains standard PDU (STP, RSTP, MSTP, LLDP, LACP) is blocked. Only PDU of STP, RSTP and MSTP protocols will be allowed to pass.

Model scheme 3

The figure shown below displays the VLAN 10 network segments located behind **SG-1** and **SG-2** and the VLAN 100 network segments located behind **SG-1** and **SG-3**.



You must connect each VLAN and enable switching of tagged frames with filtering by VLAN ID.

To do so, create a virtual switch (for example, VS-10 and VS-100) for each VLAN; for switch ports, use VLAN interfaces.

1. In **SG-1** parameters, create two VLAN interfaces (**ge-2-0-10** and **ge-2-0-100**, use the physical interface **ge-2-0** as a parent). For each VLAN interface, select **Switch port** in the **Topology** cell.
2. In **SG-2** parameters, create the VLAN interface **ge-2-0-10** (use the physical interface **ge-2-0** as a parent one). In the **Topology** cell, select **Switch port**.
3. In **SG-3** parameters, create the VLAN interface **ge-2-0-100** (use the physical interface **ge-2-0** as a parent one). In the **Topology** cell, select **Switch port**.
4. Create two virtual switches (**VS 10** and **VS 100**). In advanced parameters, select **By default**.

Note.

The **Transparent** mode is not supported in this example because the majority of the service traffic is not tagged.

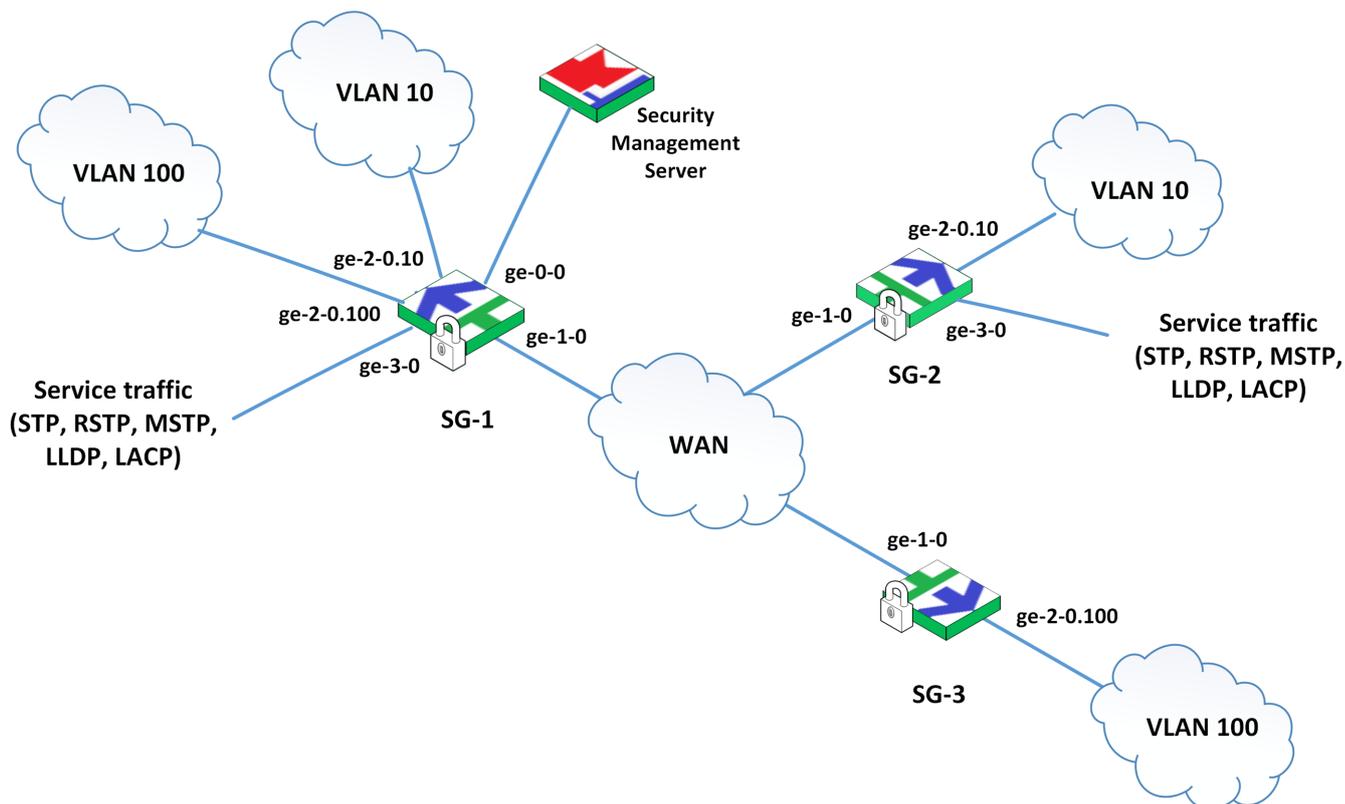
5. Add the **ge-2-0-10** interfaces of **SG-1** and **SG-2** to **VS 10**.
6. Add the **ge-2-0-100** interfaces of **SG-1** and **SG-3** to **VS 100**.

Model scheme 4

This scheme is similar to the scheme 3 and also allows service traffic to pass through **SG-1** and **SG-2**.

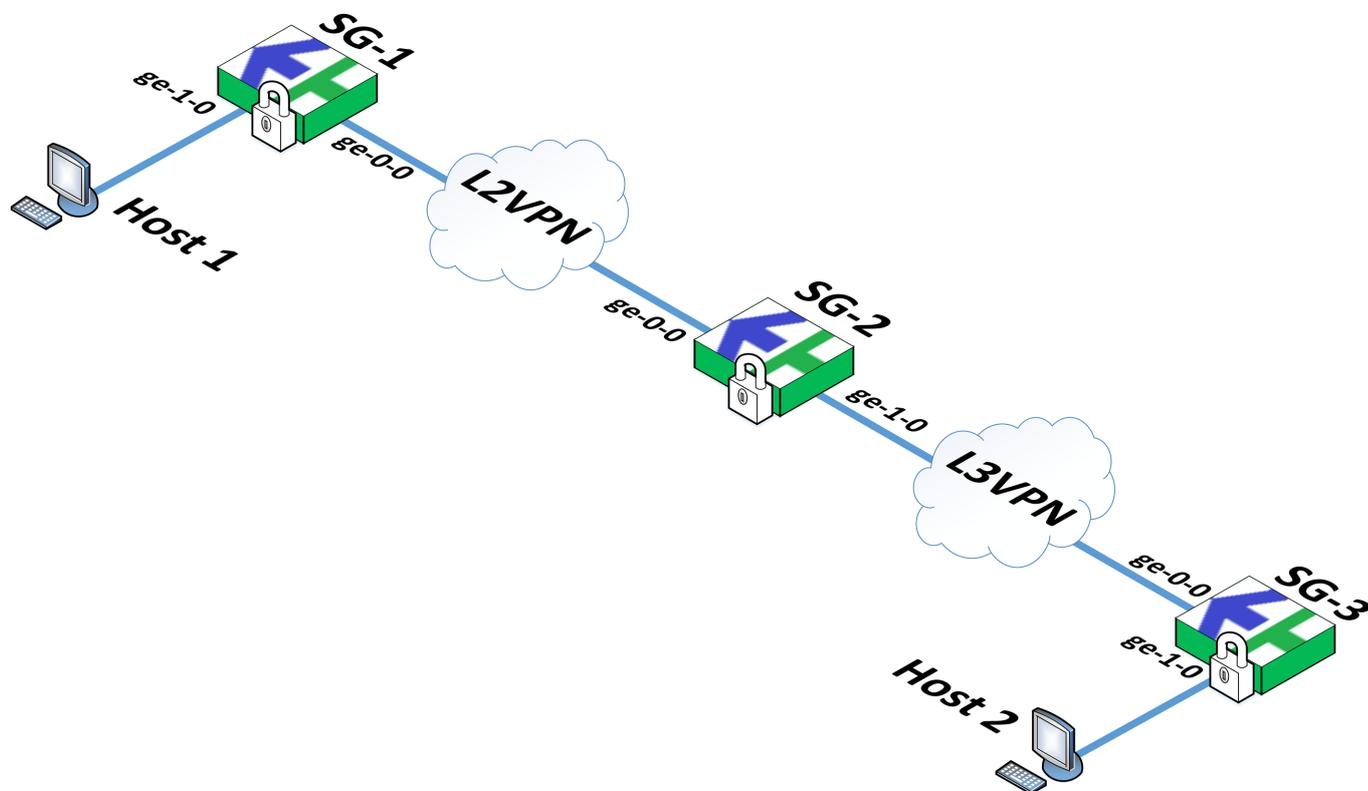
In this case, in addition to the scheme 3 configuration, do the following:

1. Create one more virtual switch (**VS 1**) for the service traffic. In the **Advanced** parameter, select **Transparent**.
2. In **SG-1** and **SG-2**, set **ge-3-0** as a switch port. The **ge-3-0** interfaces of **SG-1** and **SG-2** must be connected to the respective switch ports (see the figure below).
3. Add **ge-3-0** of **SG-1** and **SG-2** to **VS 1**.



Configure data transfer from L2VPN to L3VPN

The following scheme illustrates how traffic passes from **host 1** to **host 2** over L2VPN, then over L3VPN.



Host 1 is in the network protected by **SG-1**, **host 2** is in the network protected by **SG-3**.

SG-1 and **SG-2** are in L2VPN, **SG-2** and **SG-3** — in L3VPN.

Take the following steps to configure traffic transfer:

Step 1. Configure interfaces of SG-1

Configure interfaces:

- **ge-1-0** — switch port;
- **ge-0-0** — external, IP address — **30.1.1.101/24**.

Step 2. Configure interfaces of SG-2

1. Configure interfaces **ge-0-0** and **ge-1-0**:
 - **ge-0-0** is to connect to **SG-1**, IP address — **30.1.1.100/24**;
 - **ge-1-0** is to connect to **SG-3**, IP address — **40.1.1.100/24**.
2. On **SG-2**, create a bridge **bridge0**:
 - select **Switch port** in the **Topology** drop-down list;
 - specify the IP address of **bridge0** — **192.168.10.1/24**.

Step 3. Configure interfaces of SG-3

Configure interfaces:

- **ge-0-0** — external, IP address — **40.1.1.101/24**;
- **ge-1-0** — internal, IP address — **192.168.20.1/24**.

Step 4. Configure VPN

1. Configure L2VPN by including **ge-1-0** of **SG-1** and **bridge0** of **SG-2** in a virtual switch.
2. Configure L3VPN by adding **SG-2** and **SG-3** and the networks **192.168.10.0/24** (**SG-2**) and **192.168.20.0/24** (**SG-3**).
3. Install the Firewall rules accepting L3VPN traffic on **SG-2** and **SG-3**.
4. Install the policy on all the Security Gateways.

Step 5. Configure hosts

In network properties of hosts, specify:

Host 1

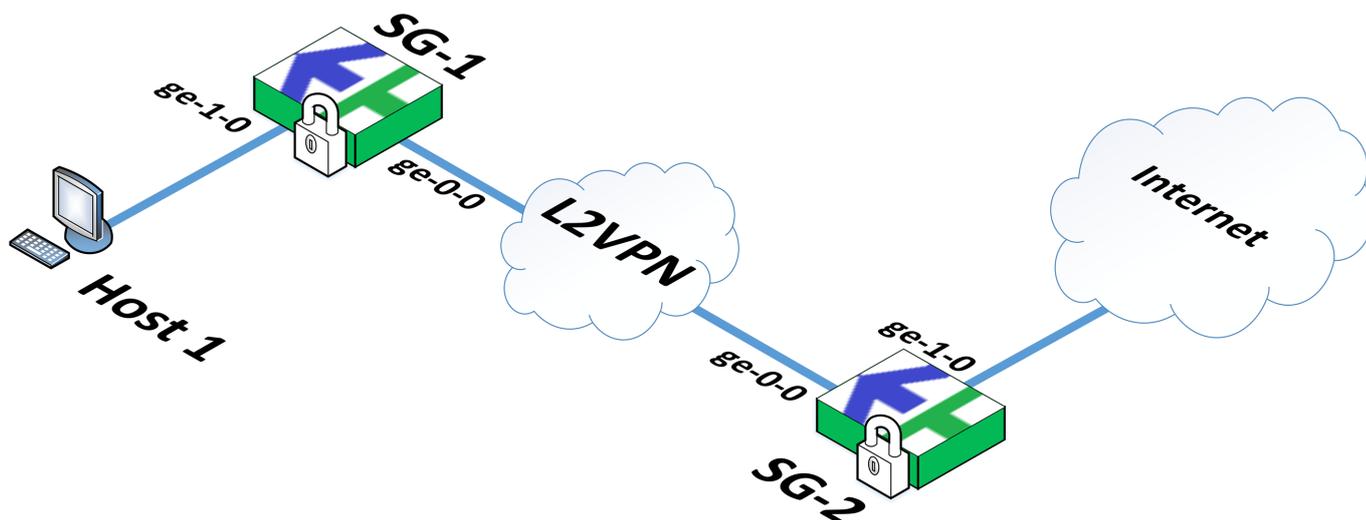
IP address	192.168.10.2/24
Default gateway	192.168.10.1

Host 2

IP address	192.168.10.2/24
Default gateway	192.168.10.1

Access to the Internet from L2VPN

The following scheme illustrates the process of gaining access to the Internet from L2VPN.



Host 1 is in the network protected by **SG-1**.

SG-1 and **SG-2** are in the L2VPN.

Take the following steps to configure access from **host 1** to the Internet:

Step 1. Configure interfaces of SG-1

Configure interfaces:

- **ge-1-0** — switch port;
- **ge-0-0** — external, IP address — **30.1.1.101/24**.

Step 2. Configure interfaces of SG-2

1. Assign **ge-0-0** with the IP address **30.1.1.100/24**.
2. On **SG-2**, create a bridge **bridge0**:
 - include **ge-2-0** in a bridge;
 - select **Switch port** in the **Topology** drop-down list;
 - specify the IP address of **bridge0** — **192.168.10.1/24**.
3. Connect **ge-1-0** to the Internet.

Step 3. Configure VPN

1. Configure L2VPN by including **ge-1-0** of **SG-1** and **bridge0** of **SG-2** in a virtual switch.
2. Install the policy on all the Security Gateways.

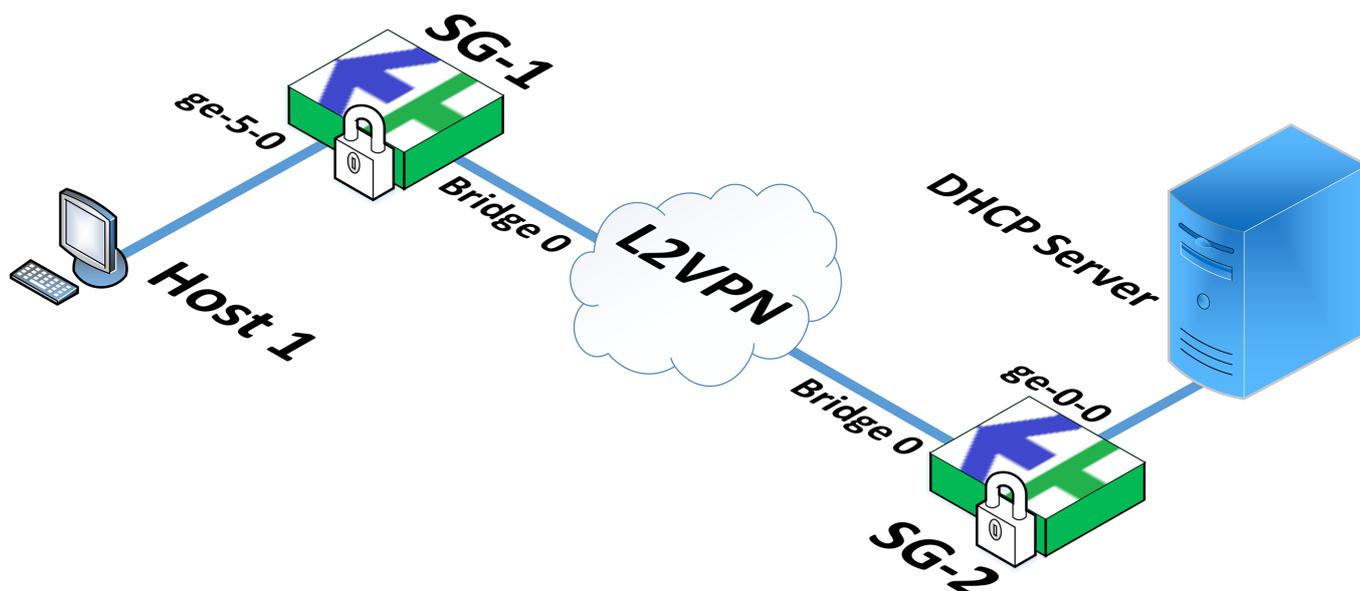
Step 4. Configure a host

In network properties of hosts, specify:

IP address	192.168.10.2/24
Default gateway	192.168.10.1

Connect to a DHCP server from L2VPN

The following scheme illustrates the process of gaining access to a DHCP server from L2VPN.



Host 1 is in the network protected by **SG-1**.

SG-1 and **SG-2** are in the L2VPN.

Take the following steps to configure access from host 1 to the DHCP server:

Step 1. Configure interfaces of SG-1

1. Assign **ge-5-0** with the IP address **9.9.9.99/24**.
2. Create a bridge **bridge0** without including a physical interface in it and assign it with the IP address **192.168.10.1/24**.

Step 2. Configure interfaces of SG-2

1. Set the **Switch port** topology for **ge-0-0** that you connect to the DHCP server.
2. Create a bridge **bridge0** and include **ge-0-0** in it.
3. Set the **Switch port** topology for **bridge0**.

Step 3. Configure a route on the DHCP server

On the DHCP server, configure a route to the network **9.9.9.0/24** over **bridge0** of **SG-1** (**192.168.10.1**).

Step 4. Select Relay mode on SG-1

1. In the Configuration Manager, open properties of **SG-1**, go to the **DHCP** section and select **Relay**.
2. In the **Relay** area, specify the IP address of the DHCP server — **192.168.10.2**.
3. Click  and select **ge-5-0** in the drop-down list.
4. Click **OK** and close the **Properties** window.

Step 5. Create a virtual switch

1. Go to **VPN | L2VPN**.
2. Create a virtual switch and include the bridge interfaces of **SG-1** and **SG-2** in it.
3. Install the policy on the Security Gateways.

Step 6. Install the policy

Install the policy on the Security Gateways.

Step 7. Configure the network adapter

On **host 1**, enable obtaining an IP address from DHCP automatically.

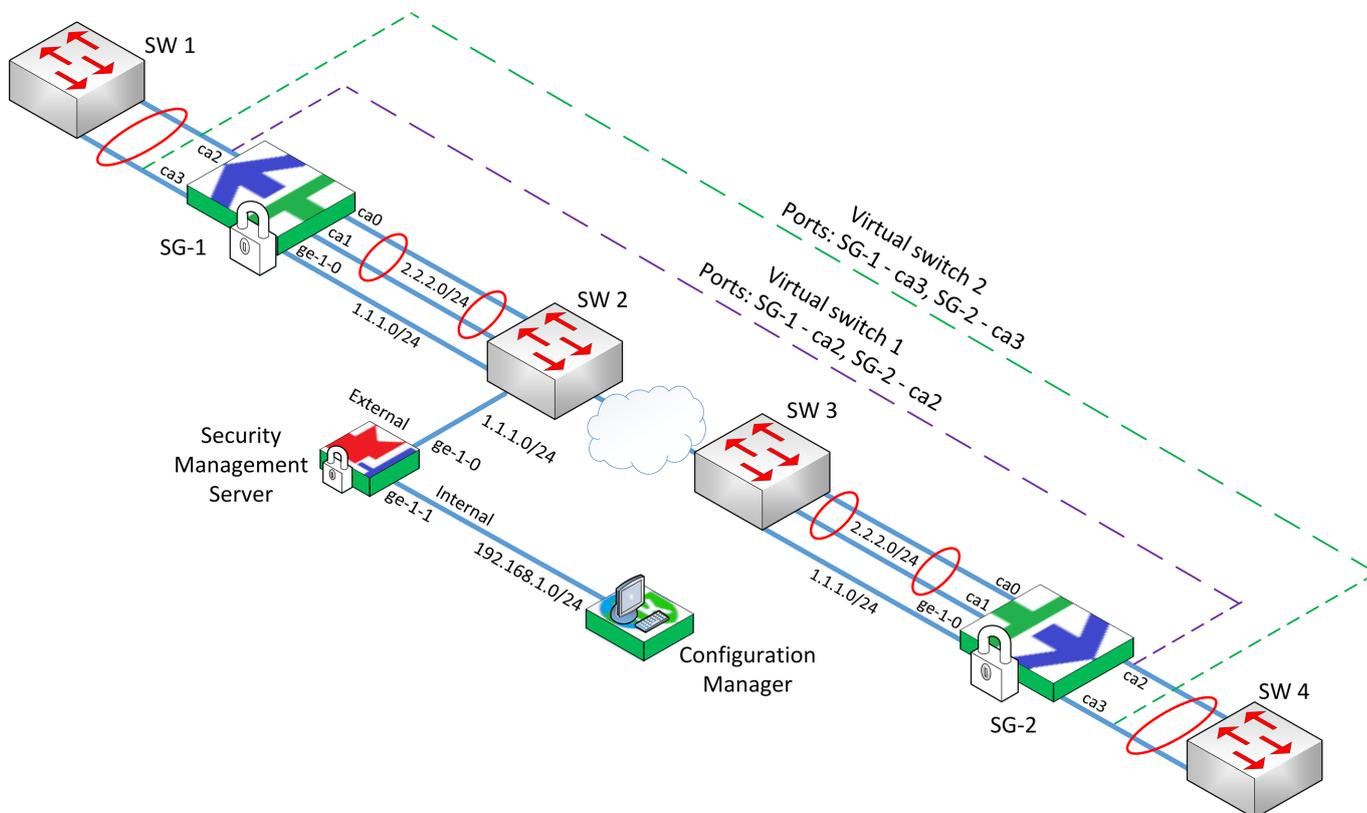
Note.

You can install the DHCP server on the Security Gateway **SG-2**. In this case, the configuration sequence of host access to DHCP server will differ from the description above as it is necessary to turn on and configure DHCP in the **Server** mode on **SG-2**. DHCP configuration is described in [5].

Scenarios for using the Security Gateway with the cryptographic accelerator

Scenario 1

The figure below illustrates a scheme of connecting the Security Gateways **SG-1** and **SG-2** to third-party equipment with bonded interfaces.



While configuring Security Gateway interfaces, the cryptographic accelerator ports **ca2** and **ca3** must be assigned **Switch port**.

A bond is configured between the switches **SW-1** and **SW-4** over a protocol passing through **L2VPN** (e.g. **LACP**). Ports **ca2** and **ca3** of the Security Gateways **SG-1** and **SG-2** are connected to the switches **SW-1** and **SW-4** respectively.

A bond is configured between switches **SW-2**, **SW-3** and external interfaces **ca0**, **ca1** of **SG-1**, **SG-2** over the **LACP** protocol.

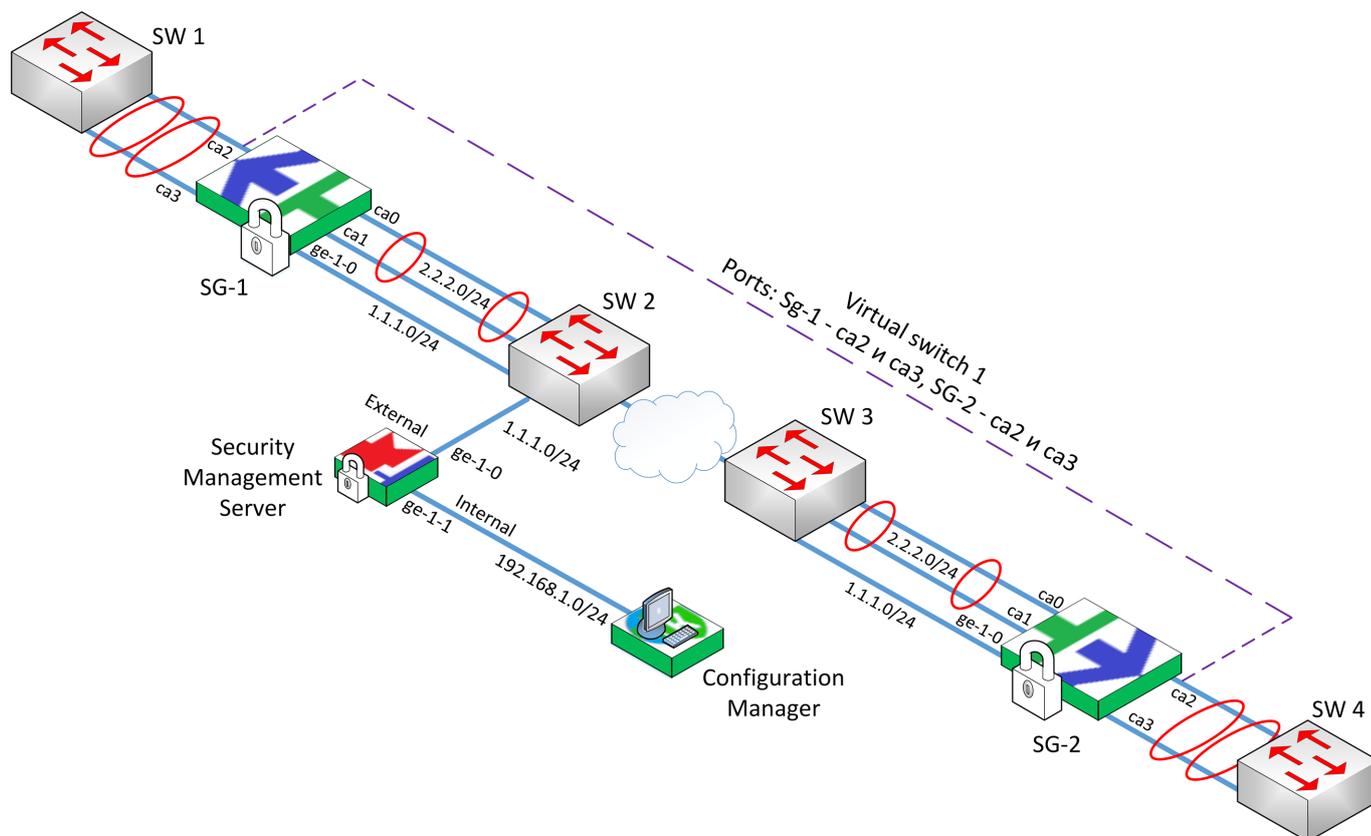
Ports **ge-1-0** are used in the Security Gateway to connect to the Security Management Server. Interface topology must be assigned **None**.

The Configuration Manager is in the subnet that is protected by the Security Gateway with the Security Management Server.

To enable **L2VPN**, create two virtual switches. Ports **ca2** must be included in the first switch, ports **ca3** — in the second switch.

Scenario 2

In this scenario, the figure below illustrates the bonding of the external interfaces **SG-1** and **SG-2** and switch ports with third-party equipment.



While configuring Security Gateway interfaces, the cryptographic accelerator ports **ca2** and **ca3** must be assigned **Switch port**.

Switch ports **ca2** and **ca3** are bonded and connected to the switches **SW-1** and **SW-4**.

External interfaces of the Security Gateways **SG-1** and **SG-2** (**ca0** and **ca1**) are bonded and connected to the switches **SW-2** and **SW-3**.

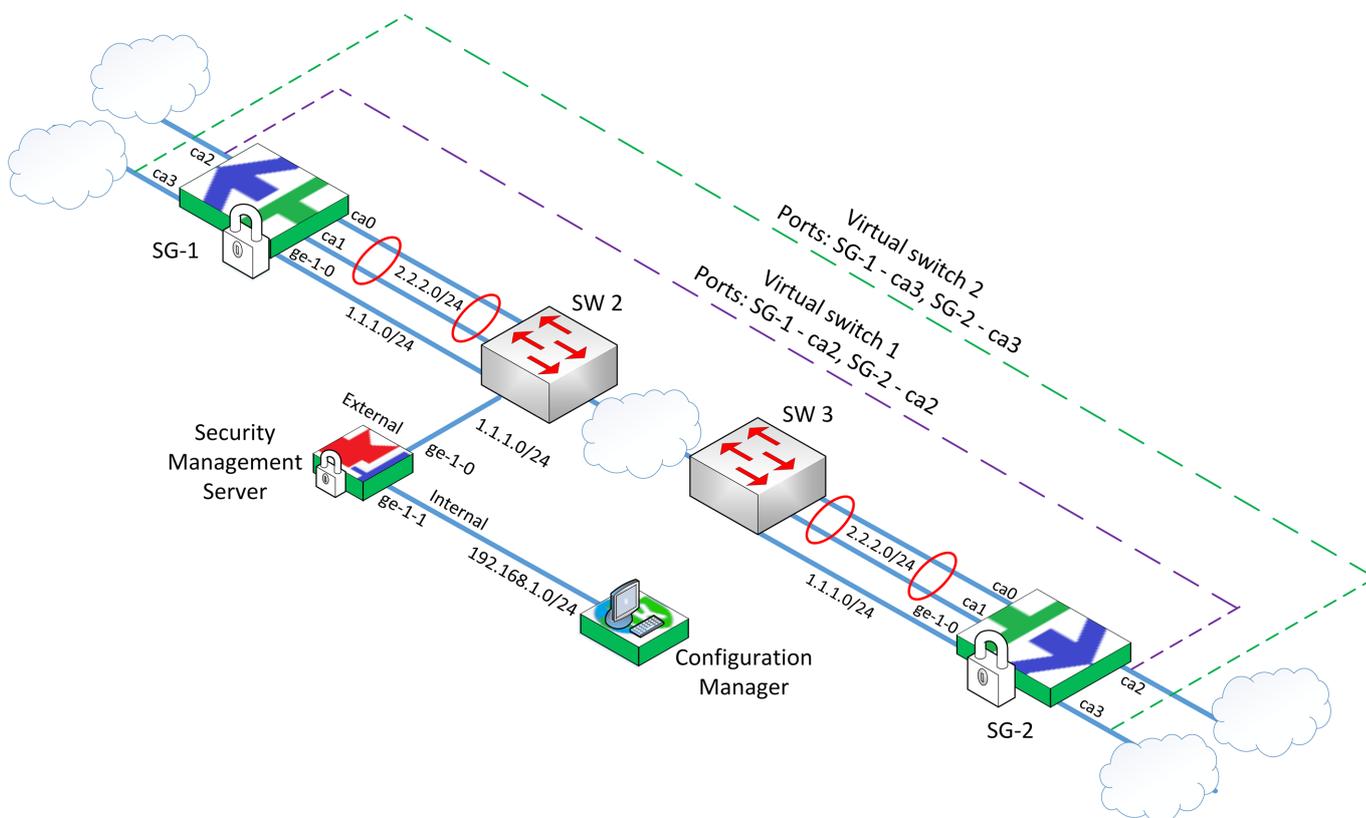
A channel bond between switches and Security Gateway interfaces is configured over the **LACP** protocol as follows:

- Switch **SW-1** and switch ports **ca1** and **ca3** of **SG-1**;
- Switch **SW-2** and external interfaces **ca0** and **ca1** of **SG-1**;
- Switch **SW-3** and external interfaces **ca0** and **ca1** of **SG-2**;
- Switch **SW-4** and switch ports **ca2** and **ca3** of **SG-2**.

To enable **L2VPN**, create a virtual switch that includes bonded switch ports **ca2** and **ca3**.

Scenario 3

In this scenario, two disjoint subnets are connected. The figure below illustrates the connection between third-party equipment and the Security Gateway interfaces **ca2** and **ca3**. A switch, a router or a host can be considered the third-party equipment.



While configuring the Security Gateway interfaces, the cryptographic accelerator ports **ca2** and **ca3** must be assigned **Switch port**.

The external interfaces **ca0** and **ca1** are bonded.

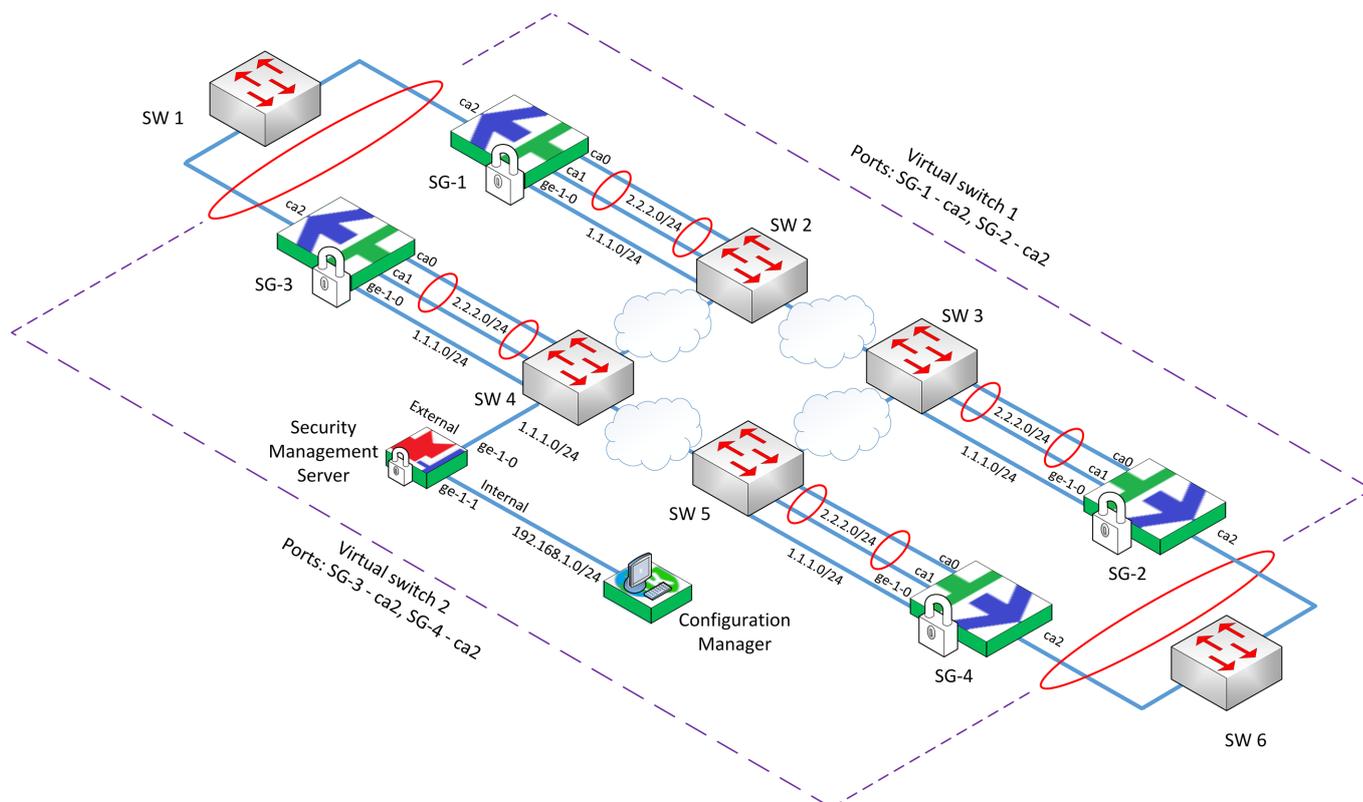
A channel bond is configured between the switches **SW-2**, **SW-3** and external interfaces **ca0**, **ca1** of **SG-1**, **SG-2** over the **LACP** protocol.

One subnet (e.g. 4.4.4.0/24) can be located outside the interfaces **ca2**. Another subnet (e.g. 5.5.5.0/24) can be located outside the interfaces **ca3**.

Ports **ca2** are included in **Virtual switch 1**. Ports **ca3** are included in **Virtual switch 2**.

Scenario 4

The figure below illustrates a scheme of connecting Security Gateways to the third-party equipment that supports **L2VPN** in case of a network device failure. The faulty network device provides traffic transfer between **SW-1** and **SW-6**.



Security Gateways **SG-1** and **SG-3** are connected to the switch **SW-1** via **ca2** ports. Security Gateways **SG-2** and **SG-4** are connected to **SW-6** in the same way.

While configuring Security Gateway interfaces, the cryptographic accelerator ports **ca2** must be assigned **Switch port**.

The external interfaces **ca0** and **ca1** are bonded and connected to the switches **SW-2** – **SW-5**.

A channel bond is configured between the switches **SW-1** and **SW-6** over a protocol passing through **L2VPN** (e.g. **LACP**). The external failover channels are based on the third-party equipment.

A channel bond between switches and Security Gateway external interfaces (**ca0** and **ca1**) is configured over the **LACP** protocol as follows:

- Switch **SW-2** and **SG-1**;
- Switch **SW-3** and **SG-2**;
- Switch **SW-4** and **SG-3**;
- Switch **SW-5** and **SG-4**.

Ports **ca2** of **SG-1** and **SG-2** are included in **Virtual switch 1**. Ports **ca2** of **SG-3** and **SG-4** are included in **Virtual switch 2**.

In case of a device failure, all the traffic between **SW-1** and **SW-6** is transferred to the devices corresponding to another virtual switch.

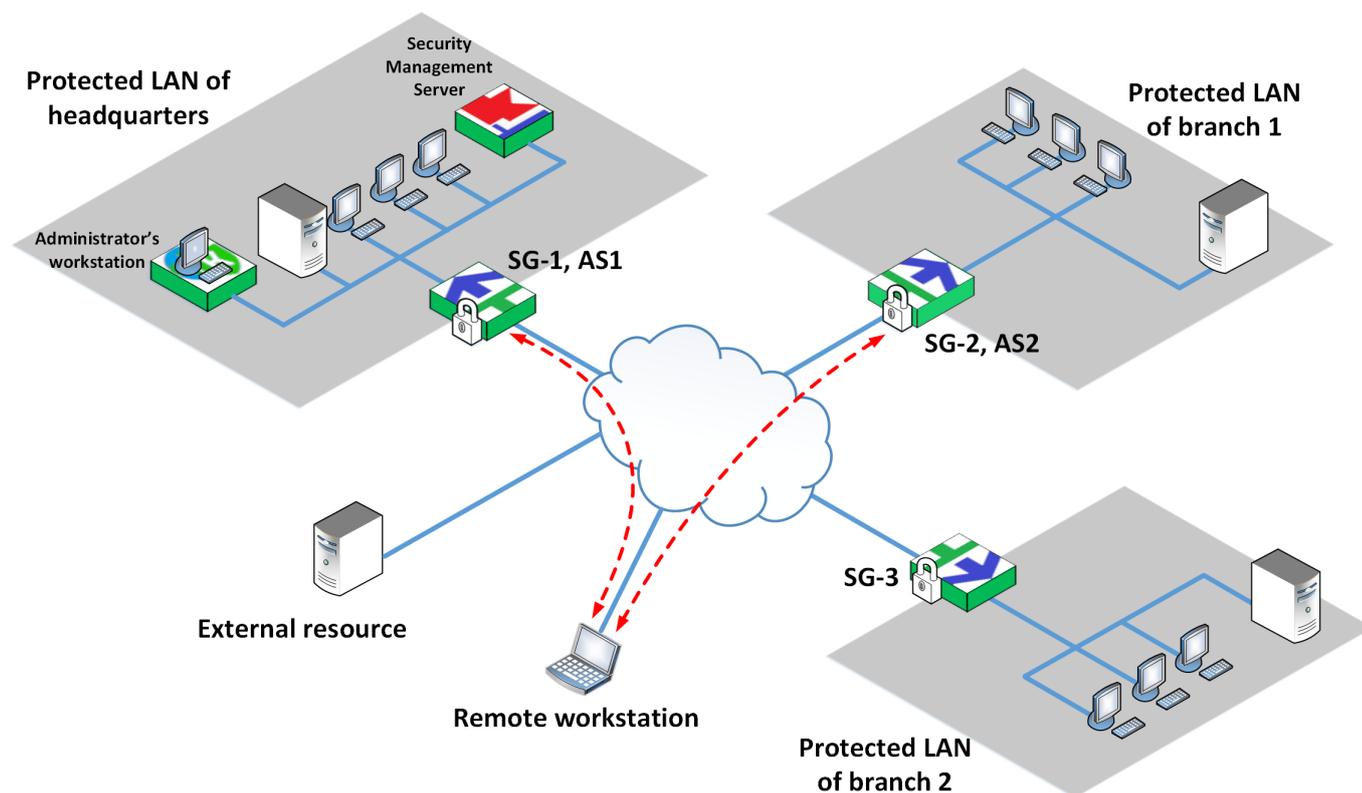
Chapter 5

Remote access

Overview

Continent Enterprise Firewall includes tools providing users of remote workstations (hereinafter — remote users) that are not part of protected network segments with remote access to VPN resources.

Access Server is a software component of Continent Security Gateway. The additional software component Continent-RA installed on a remote user's workstation allows remote users to connect to an Access Server and provides them with access to resources of a protected network.



The Access Server provides its services only to protected networks of the Security Gateway on which it is installed. A remote user signed on several Access Servers may connect to any of them from every workstation on which Continent-RA was installed. Simultaneous connection to several Access Servers from one workstation with Continent-RA is not supported.

Connection between a remote user and protected network users is based on public data networks.

A remote user can initiate and terminate a connection between Continent-RA and the Access Server. Both the user and the administrator can terminate the connection. The Access Server can terminate a session automatically after changing the Security Gateway configuration.

A secure connection (with encrypted traffic) can be established between a workstation with Continent-RA and the Access Server only after its mutual authentication that can be performed by password or certificate based on x509v3 public keys. However, password and certificate transfer is encrypted.

After the connection is established, the Access Server sends the list of routes available for a user to Continent-RA. All traffic exchanged between a workstation with Continent-RA and a secure network is encrypted by the TLS.

The Access Server assigns the workstation with Continent-RA with a private IP address from a previously created IP address pool. The IP address can be dynamic or static. After that, a user can access the protected network only using this IP address.

Access Server

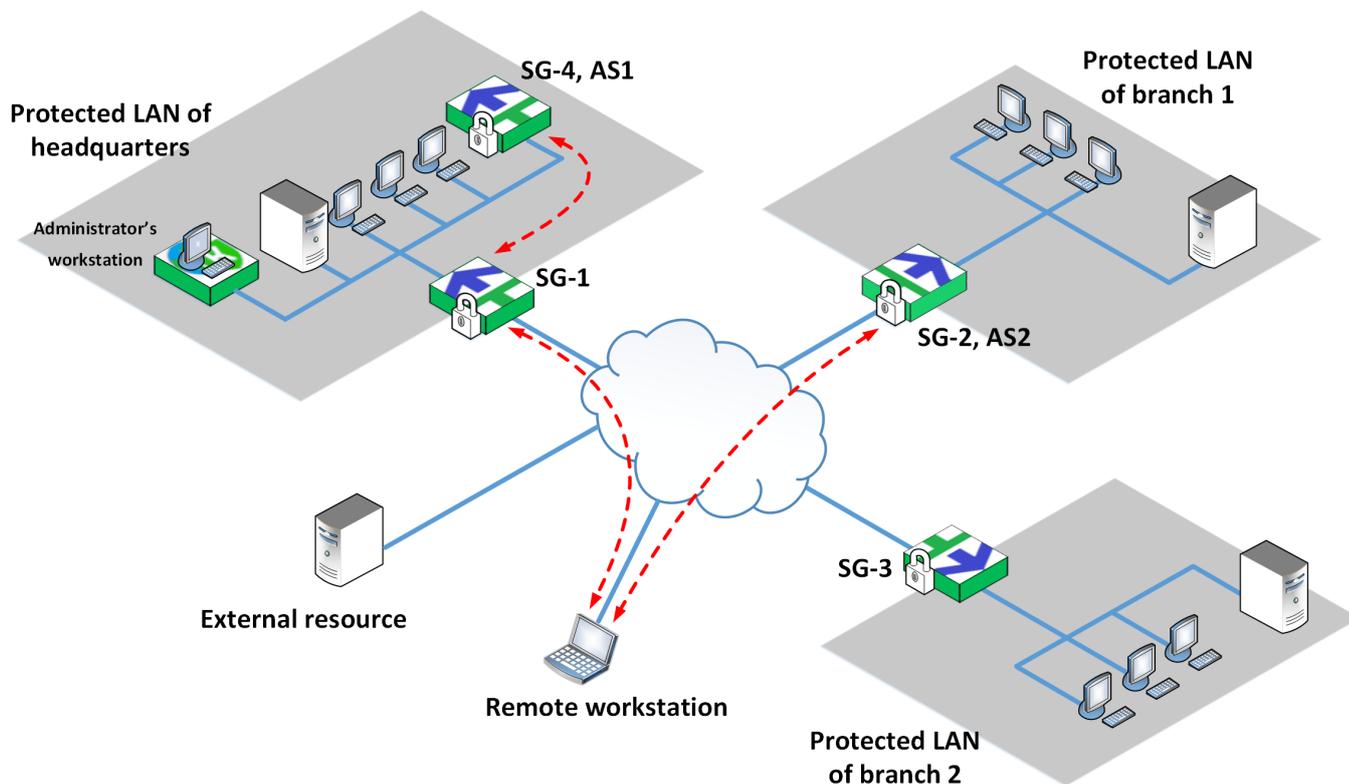
The Access Server provides:

- secure connection between an exchange point and a network protected by the Security Gateway;

- remote users authentication via public key x509v3 certificates;
- filtering rules upload to the Security Gateway IP packets filter respectively to the rights of a connected user;
- the control of secure connections between Continent-RAs and the Security Gateway. Session information upload upon disconnection;
- server, management program use and remote user connection event logging.

The Access Server can be installed on a Security Gateway protecting a corporate network perimeter (see the figure on p. 56) or on a Security Gateway within a protected network.

In the figure below, you can see the Access Server **AS1** that is installed on the Security Gateway **SG-4** within the protected network of the headquarters.



Continent-RA

Continent-RA includes:

- Continent-RA management program;
- Security Code CSP;
- Continent-RA Integrity Check application;
- Collection of diagnostic information application.

Continent-RA can perform the following:

- establish a secure connection and encrypted data exchange with the Access Server;
- log operation events;
- manage a Public Key Infrastructure (PKI);
- control the integrity of the software, transferred and stored information.

Continent-RA supports the following connection management modes;

- No restrictions — all connections are allowed for a workstation with Continent-RA installed.
- Unsecure connections prohibited — all unsecure connections (ones that are not allowed by remote access rules of the Access Server) are prohibited during communication with the protected network resources.
- All connections are redirected through the tunnel between the Continent-RA and the Access Server.

Access control

Remote users' access is managed by remote access rules. The rules define remote users' access rights to protected network resources that are specified as network objects (hosts, subnets). You can set an authentication method (by password or by certificate) for the connection between the Access Server and Continent-RA as well as the management mode of Continent-RA connections. Apart from that, in the rule, you need to specify a Security Gateway on which the Access Server is deployed and to which the rule is applied.

A set of rules comprises a remote access policy. Remote users gain access rights to protected network resources respectively to a remote access policy.

An administrator creates remote access rules via the Configuration Manager. After a remote access policy is applied, the rules are applied to specified Security Gateways.

As Continent-RA connects to a Security Gateway (Access Server), a remote user is authenticated according to a remote access rule applied to the Security Gateway.

After mutual authentication is completed, a secure connection between the Access Server and Continent-RA is established. The Access Server transfers to Continent-RA parameters and the list of routes that is based upon a remote access rule. Upon passing through the tunnel, Continent-RA packets are processed by a Security Gateway and are redirected to the required resource respectively to applied filtering rules.

Certificate-based user authentication

A remote user is authenticated via public key X.509v3 certificates.

A certificate contains an owner's name, his or her public key, and additional system information. This information is validated by the signature of a trusted certificate authority.

The following certificates are used: a root certificate, an Access Server certificate and a user certificate.

Certificates can be issued in two ways:

- By a trusted certificate authority. A certificate authority issues a root certificate, an Access Server certificate, as well as users certificates. To issue an Access Server certificate, an administrator must make a request via the management program. To issue a user certificate, a request must be made via Continent-RA. An administrator cannot access a certificate authority private key and user certificate private keys. Issued certificates are registered on the Access Server and then transferred to users.
- By the Security Management Server as a trusted certificate authority. An administrator issues a root certificate, an Access Server certificate and user certificates using the Configuration Manager and the cryptographic service provider. An Access Server certificate and user certificates are signed with the certificate authority private key, that is, with the Security Management Server private key.

User certificates can be issued via Continent-RA as well. In this case, an administrator cannot access users' private keys.

The Security Management Server and Continent-RAs include a cryptographic service provider.

Several root certificates and several Access Server certificates can be used simultaneously. Each user can also have several certificates. Different certificates can be signed with different certificate authority private keys or with the private key of the same certificate authority. In case of a planned certificates change, this option allows you to register new certificates before the expiration date of the replaced ones. We recommend registering reserve certificates in case an emergency happens. For example, if the private key of a certificate authority is compromised.

When certificates are changed, users connected to the Access Server can continue to work until they log out. If it is necessary to update certificates because of a possible compromising, all users must be automatically disconnected from the Access Server after certificates are changed.

Access Server management

To provide remote users with access to protected network resources, configure the Access Server by specifying DNS servers, domains and the range of addresses that are assigned to Continent-RAs when connecting to the Access Server.

An administrator configures the Access Server via the Configuration Manager.

Remote access configuration

Before configuring remote access, make sure the following is done:

- On Security Gateways, routes providing remote users with access to protected network resources are specified.
- Security Gateways with Access Servers installed are enabled.

Note.

To activate the **Access Server** component, the respective license is required.

Configuration must be performed in the following order:

1. Certificates issue (see below).
2. Creating the list of users to provide with remote access (see p. 60), export Continent-RA profiles and Continent-RA user profiles.
3. Access Server enabling and configuration (see p. 61).
4. Set remote access rules (see p. 66).

Certificates

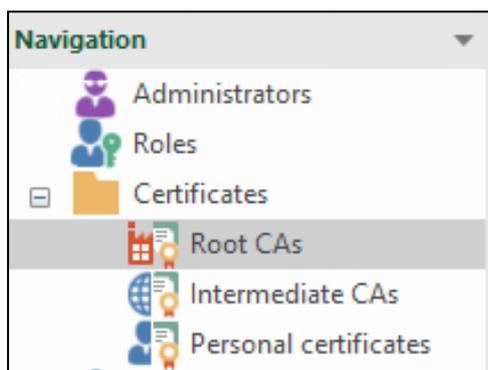
The following three certificates are used when authenticating a user on the Access Server: an Access Server certificate, a root certificate, a user certificate. If authentication by password is used, a user certificate is not in use.

Certificates are issued via the Configuration Manager. Certificates issued by a third party certificate authority can be imported.

To issue a certificate:

1. In the Configuration Manager, go to **Administration** and expand **Certificates**.

The **Certificates** folder contains three certificate categories.



2. Select the required category:
 - to issue a root certificate, select **Root CAs**;
 - to issue an Access Server certificate, select **Personal certificates**.

The list of certificates appears in the display area. If you have not created certificates before, the list is empty.

Certificates (3)				
Search...				
Name	Issued by	Valid from	Valid to	Status
????????? ??????? ??	????????? ??????...	30.05.2017 13:34	30.05.2028 13:44	Valid
Root_cert	Root_cert	20.09.2022 08:55	19.09.2027 08:55	Valid
test	test	20.09.2022 09:39	20.09.2027 10:38	Valid

3. Click **Certificate** on the toolbar.
The respective dialog box appears.

4. Select **Access Server** in the **Certificate type** drop-down list, specify the required parameters and click **Create certificate**.

Attention!

While creating an Access Server certificate, enter the Access Server IP address or its DNS name in the **Common Name** field. DNS name must be entered in English without spaces, it can contain digits, symbols "." and "-". The name cannot start and end with "." and "-". The maximum number of symbols is 256.

The created certificate appears in the list.

User list

The list of users that you need to provide remote access to a Security Management Server object and can be created in the Configuration Manager. User groups imported from Active Directory can be added to the list.

Note.

For more information about Security Management Server objects and importing accounts from Active Directory, see [2].

To view a list:

1. In the Configuration Manager, go to **VPN**.
The **Objects** display area appears.
2. Select .

Name	Full name	Description
 j.doe	John Doe	Network administrator
 w.gates	William Gates	Security administrator

The list contains users and user groups created in the Security Management Server, as well as user groups imported from the Active Directory. If no users have been created, the list is empty.

Attention!

If user authentication on an Access Server is intended to be by certificate, issue a personal certificate. You can issue a personal certificate either while adding a new user or later.

To add a new user to the list:

1. Right-click the display area and select **Create**.
The **User** dialog box appears.

User

General information | Authentication | User groups

Login:

Full name:

Description:

Email:

Organization:

Position:

Block the account

OK Cancel Apply

2. In the **General information**, configure the account parameters according to [2].
3. If it is necessary, create a personal certificate by clicking **Authentication** and enter the required data — **Password** and **Certificate** (see [2]).

If the user authentication by certificate is planned, click  and select the required certificate.

If there is no respective certificate, click **Create certificate** and perform the required steps.

4. If it is necessary, create a group and add required users to it.
5. After configuring all the parameters, click **OK**.

The **User** dialog box closes and the new user is added to the list.

To connect a new user to the network, export the Continent-RA user profile and the Continent-RA profile. The Continent-RA user profile contains data for connecting to the Continent-RA, server certificate and user certificate. The Continent-RA profile contains the data for connecting to the Continent-RA and the server certificate. For detailed information about exporting Continent-RA and user profiles, see p. 67.

Configure the Access Server

You can configure the Access Server in the Configuration Manager.

To configure the Access Server:

1. Go to **Structure**, select the Security Gateway on which you want to enable and configure **Access Server** and click **Properties** on the toolbar.

The respective dialog box appears.

2. In the **Components** group box, select **Access Server**.

The respective section appears on the left.

Note.

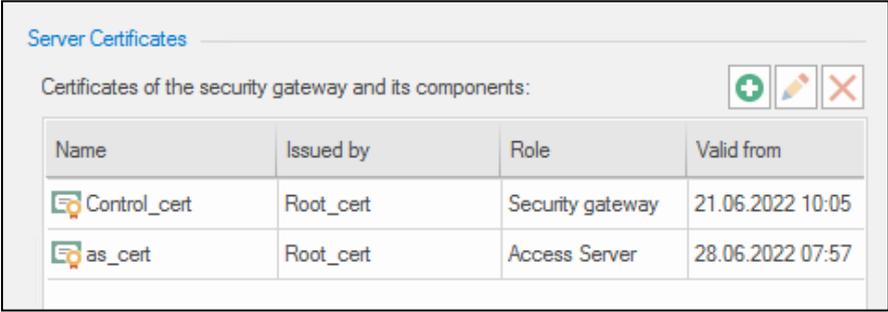
When you select **Access Server**, **User Identification** is selected automatically. On the left, the **User Identification** section appears. You do not need to configure **User Identification**.

3. On the left, select **Certificates**.

Server and root certificates appear on the right.

4. In the **Server Certificates** section, click **Add certificate** and in the drop-down list, select the respective Access server certificate.

The Access server certificate will be added to the Server certificate list.



The screenshot shows a dialog box titled "Server Certificates" with a subtitle "Certificates of the security gateway and its components:". It features a table with four columns: Name, Issued by, Role, and Valid from. There are two rows of data. Above the table are three icons: a plus sign, a pencil, and a red X.

Name	Issued by	Role	Valid from
Control_cert	Root_cert	Security gateway	21.06.2022 10:05
as_cert	Root_cert	Access Server	28.06.2022 07:57

5. On the left, select **Access Server**.

The respective parameters appear on the right.

6. In the **Listen on port** field, specify the port to connect to the Access Server. Port 443 is specified by default.
7. In the **Maximum inactive session timeout** field, specify the time to wait for an inactive session in seconds. 60 seconds is the default value.
8. If you need to allow traffic between users/user groups, select the respective check box. In this case, new routes will be added to make it possible to transfer traffic between all users of the Access Server.
9. If you need to optimize the performance of the Access Server, select the respective check box.

Note.

In this mode, the IP address pool specified below will be divided into several smaller subnets,

The optimization mode is only supported for IP address pools with a subnet mask from 19 to 27.

Attention!

For correct operation of the **Allow traffic between users** option if the optimization mode is enabled, create a remote access rule, allowing user access to a subnet of the user IP address pool specified in the Access Server properties (see p. 66).

10. Enter the IP addresses of DNS servers of the protected network in the respective fields.

Attention!

At least one DNS server must be specified.

11. Specify an address pool for workstations with Continent-RA by clicking the **Create a new IP address pool** button.
 - If the optimization mode was not enabled, a new dialog box will look like this:

Access Server IP Address Pool

IP address pool: ⓘ

Pool addresses

Default gateway: /

IP address range: –

Available addresses:

Users

Users and user groups address assignment: + ✎ ✖

Groups/Users	Address
ⓘ No items found.	

OK Cancel

Go to **12**.

- Otherwise, the dialog box will look like this:

Access Server IP Address Pool

IP address pool: ⓘ

Pool addresses

List of address pool tunnels:

Gateway	Subnet mask	Address range		Amount	
		First	Last	Free	Total
192.168.217.1	255.255.255.224	192.168.217.2	192.168.217.30	29	29
192.168.217.33	255.255.255.224	192.168.217.34	192.168.217.62	29	29
192.168.217.65	255.255.255.224	192.168.217.66	192.168.217.94	29	29
192.168.217.97	255.255.255.224	192.168.217.98	192.168.217.126	29	29

Users

Users and user groups address assignment: + ✎ ✖

Groups/Users	Address
ⓘ No items found.	

OK Cancel

Go to **16**.

- 12.** To specify an IP address pool, enter the IP address and subnet mask.

The fields below will be filled in automatically.

- 13.** To distribute IP addresses among users, in the **Users** section, click the **Add** button.

The list of the users appears.

- 14.** Select users/user groups for whom you want to assign the IP address pool and click **OK**.

The selected users are displayed in the **Users** section of the **Access Server IP Address Pool** dialog box with either the dynamic or the static method of IP address assignment. By default, a user/user group is assigned a dynamic address from the pool. In this case, you can see the **Automatic** value in the **Address** column.

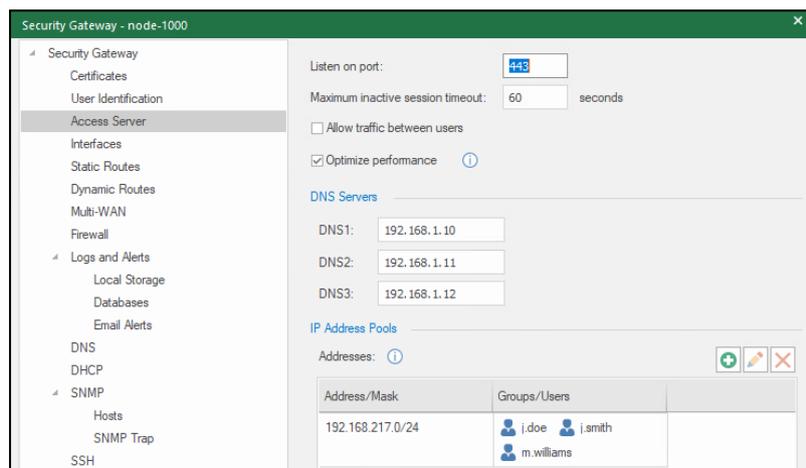
If you want to assign a static IP address to a user, click the respective Address cell and enter an IP address from the pool.

Attention!

The IP address must be unique for each user within one Access Server.

- 15.** Click **OK** in the **Access Server IP Address Pool** dialog box.

You will be returned to **Access Server**. If necessary, add other IP address pools.



If necessary add more addresses pool. Go to **20**.

- 16.** Specify an IP address pool.

The pool will be divided automatically into subnets. A list of tunnels will be created as well.

- 17.** To distribute IP addresses among users and user groups, in the **Users** section, click the **Add** button.

A dialog box with a list of registered users appears.

- 18.** Select users/user groups for whom you want to assign the IP address pool and click **OK**.

The selected users are displayed in the **Users** section of the **Access Server IP Address Pool** dialog box.

- 19.** Click **OK**.

You will be returned to **Access Server**. If necessary, add other IP address pools.

- 20.** After you have added all the IP address pools, select one of them as a pool to connect users imported from Active Directory. For this purpose, specify it in the **Pool to connect users from LDAP** field.

- 21.** After the Access Server configuration, click **Apply** or **OK**.

- 22.** Install a policy on the Security Gateway with the configured Access Server.

Configure an Access Server security cluster

To configure an Access Server cluster using the Configuration Manager:

- 1.** Go to **Structure**.

The list of Security Gateways appears in the display area.

- 2.** Select the first Security Gateway that is included in the security cluster and select **Properties** on the toolbar.

- 3.** On the left, select **Certificates**.

- 4.** Click **Add certificate** and in the drop-down list, select the respective Access Server certificate.

The Access Server certificate will be added to the Server certificate list.

Server Certificates

Certificates of the security gateway and its components:

Name	Issued by	Role	Valid from
Control_cert	Root_cert	Security gateway	21.06.2022 10:05
as_cert	Root_cert	Access Server	28.06.2022 07:57

5. Perform the same actions for the second Security Gateway.

Attention!

To ensure correct operation of the Access Server, on the security cluster, create two certificates with the same names. Then, add the first certificate to the first Security Gateway, and the second certificate to the second Security Gateway.

6. Select the required security cluster and click **Properties** on the toolbar.

The respective dialog box appears.

7. In the **Components** group box, select **Access Server**.

The respective section appears on the left.

Note.

When you select **Access Server**, **User Identification** is selected automatically. On the left, the **User Identification** menu item appears. You do not need to configure User Identification.

8. On the left, select **Access Server**.

The respective parameters appear on the right.

DNS Servers

DNS1: 192.168.1.10

DNS2: 192.168.1.16

DNS2: 192.168.1.17

Domain: securitycode.ru

Continent-RA Addresses

Addresses: ⓘ

Address/Mask
10.0.0.0/24

OK Cancel Apply

9. Enter IP addresses for DNS servers and a domain of the protected network in the respective fields.

10. Specify an address pool for workstations with Continent-RA by clicking  and specifying an address and a mask.

11. On the left, select **Cluster**.

The cluster parameters appear on the right.

12. Configure the cluster parameters according to the instruction (see [3]).

13. After you finish configuring **Access Server**, click **OK** or **Apply**.

Remote access rules

You need to install a rule that defines Continent-RA user access to the corporate protected resources on the Access Server. There are the following conditions:

- List of users or groups with granted access.
- Authentication method (by certificate, by password, by certificate or password).
- List of resources (network objects) to which access is granted.
- Connection control mode.

There are three connection control modes:

Name	Description
Deny unsecured connections	For Continent-RA and Access Server, prohibits all connections except access to protected resources specified in a remote access rule
Redirect through tunnel	Redirects all Continent-RA traffic to an Access Server
No control	During a connection session of Continent-RA and Access Server, all other connections are permitted

- Multiple connections control (allow/restrict establishing connection under one account from multiple computers at the same time).
- Timeframe (rule validity period).
- List of Access Servers on which the rule is installed.

Each rule has its own sequence number, name and description.

An Access Server may have several rules installed.

Attention!

You need to install the Firewall rules on the Security Gateway. These rules are required to allow remote users to work with protected resources.

To view the list of rules:

- In the Configuration Manager, go to **VPN**, and select **Remote access**.

The list of rules appears in the display area.

No.	Name	Users	Authentication m...	Access	Connection control	Install On	Description
1	Mail	j.doe w.gates	Password	All_Net	No control	SG-1	
2	Portal	j.doe w.gates	Password	All_Net	Deny unsec...	SG-1	
3	Access Server	w.gates	Certificate		Redirect thr...	SG-1	

If there are no rules, the list is empty.

Note.

Use the list of rules according to the description for the Firewall rules (see [2]).

To create a rule:

1. In **Remote access**, click the required rule button in the **Create** group of the toolbar.
The created rule appears in the list.
2. Select a required parameter and specify its value. For **Name** and **Description**, specify values by entering them in the respective text boxes, for others — by selecting them in the drop-down lists.

Attention!

The users must not be in more than one remote access rule at the same time. This restriction also applies to users belonging to groups and the users imported from Active Directory.

3. After you finish configuring rule parameters, save the changes.

Export Continent-RA profiles

To connect a new user, export RA profiles and RA user profiles.

An RA profile contains data required to connect to the Access Server and a server certificate. The RA user profile contains data required to connect to the Access Server, a server and personal certificates.

To export the Continent-RA profile:

1. In the Configuration Manager, go to **Access Control** or **VPN**.
2. In the Security Management Server object list, select **Users**.
3. Right-click a required user and select **Export | Configuration profile for Continent RA**.

The **Export profile for Continent-RA** dialog box appears.

The screenshot shows the 'Export profile for Continent-RA' dialog box. The title bar is green with a close button. The main content area is light gray and contains the following elements:

- Access server:** A section with a green icon and the text 'The list of Access Servers to connect'. Below it, a list of servers is shown with 'node-10' selected and underlined. To the right of the list are '+' and 'X' buttons.
- Name:** A text input field containing 'node-10'.
- Domain:** A text input field containing 'domain-10'.
- Certificate:** A dropdown menu.
- Ports:** A section with two input fields: 'TCP:' containing '443' and 'UDP:' containing '4433'.
- Extra:** A section with two checkboxes:
 - Make the connection to the default server
 - Allow connection to user logon
- Navigation:** At the bottom, three buttons: '< Back', 'Next >', and 'Cancel'.

Note.

If the only Access Server is registered in the Configuration Manager, it is selected automatically. To add an Access Server, click .

4. If necessary, select the additional options:
 - Make the connection to the default server;
 - Allow connection to user logon.
5. Click **Next**.
6. Specify **File name**.
7. To select a file saving path, click  and specify the path in the Windows explorer.
8. Enter and confirm the password.
The **You have successfully exported the profile** message appears.
9. Click **Done**.
The Continent-RA profile is ready to be imported to Continent-RA.

To export the Continent RA user profile:

1. In the Configuration Manager, go to **Access Server** or **VPN**.
2. In the Security Management Server object list, select **Users**.
3. Right-click a required user and select **Export | User profile for Continent RA**.
The **Select the user certificate** dialog box appears.
4. In the drop-down list, select a certificate and click **Next**.
5. Add Access Servers and select the additional options if necessary:
 - Make the connection to the default server;
 - Allow connection to user logon.
6. Click **Next**.
7. Specify **File name**.
8. To select a path to save a file, click  and specify the path in the Windows explorer.
9. Enter and confirm the password.
The **You have successfully exported the profile** message appears.
10. Click **Done**.
The Continent-RA user profile is ready to be imported to Continent-RA.

Documentation

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