Documentation of FW Operation for the KISG

KasperskyOS Products

Exported on Nov 15, 2021

Table of Contents

1 Abbreviations 4

2 Introduction 5

3 Description of the firewall operation 6
3.1 Description of network segments 6
3.2 FW rule sources 7
3.3 Application of FW rules 8
3.3.1 Resultant FW rule policy 8
3.3.2 Current service rules of access to the MQTT, KSC, and Syslog (SystemRules) 9

4 Specifics of the IDS/IPS operation 11
4.1 Function of the IDS component within the KISG 11
4.2 Analysis of IDS/IPS events 11
4.3 Work with blocked IP addresses. The BlockedListRules list and adding exceptions to the AllowListRules list for the IDS 12
4.4 Improvement of detection quality 13

5 Examples of the KISG firewall application for various implementation schemes 14
5.1 Preparation for access control 14
5.2 Implementation scheme with NAT enabled in the KISG 14
5.2.1 Access control for a host from the LAN zone with the KISG running in the NAT mode 15
5.2.2 Blocking a host after an IDS event 16
5.3 Implementation scheme with the KISG running in the packet routing mode 17
5.3.1 Routing 18
5.3.2 Access control for a host from the WAN zone with the KISG running in the routing mode 19
5.3.3 Adding a deny rule for a host from the WAN zone with the KISG running in the routing mode 19
5.3.4 Access control for a host from the LAN zone with the KISG running in the routing mode 20
5.4 KISG configuration in the modem mode 21

6 Identification of a matching implementation scheme 22

- Abbreviations
- Introduction
- Description of the firewall operation
  - Description of network segments
  - FW rule sources
  - Application of FW rules
    - Resultant FW rule policy
    - Current service rules of access to the MQTT, KSC, and Syslog (SystemRules)
- Specifics of the IDS/IPS operation
  - Function of the IDS component within the KISG
  - Analysis of IDS/IPS events
  - Work with blocked IP addresses. The BlockedListRules list and adding exceptions to the AllowListRules for the IDS
  - Improvement of detection quality
- Examples of the KISG firewall application for various implementation schemes
  - Preparation for access control
  - Implementation scheme with NAT enabled in the KISG
    - Access control for a host from the LAN zone with the KISG running in the NAT mode
    - Blocking a host after an IDS event
  - Implementation scheme with the KISG running in the packet routing mode
    - Routing
    - Access control for a host from the WAN zone with the KISG running in the routing mode
    - Adding a deny rule for a host from the WAN zone with the KISG running in the routing mode
    - Access control for a host from the LAN zone with the KISG running in the routing mode
  - KISG configuration in the modem mode
- Identification of a matching implementation scheme

1 Abbreviations

KISG – Kaspersky IoT Secure Gateway

IDS – Intrusion detection system

IPS – Intrusion prevention system

LAN – Interior zone with respect to the KISG

WAN – Exterior zone with respect to the KISG

FW – Firewall

IS – Information security

NAT – Network Address Translation

KSC –Kaspersky Security Center server

SSH – Secure Shell (an application layer network protocol which allows secure remote control)

HTTP – HyperText Transfer Protocol

MQTT – Message queuing telemetry transport (a simplified network protocol running over TCP/IP focused on inter-device message exchange based on the publisher–subscriber concept)

PPP – Point-to-Point Protocol (a data link layer two-point protocol)

2 Introduction

This manual is intended to familiarize professionals implementing the Kaspersky IoT Secure Gateway (KISG) with the specifics of the Firewall (FW) configuration depending on the KISG implementation scheme. This manual gives instructions for the following procedures:

- Setup of the network accessibility for hosts located within the various segments of the KISG.
- Analysis of IS events.
- Editing firewalling rules.

The firewall within the KISG is intended to filter out forbidden traffic. The FW with a fixed set of rules blocks unwanted network connections, which reduces the probability of potentially malicious networking via the KISG, while the IDS/IPS provides identification of the basic network attacks on the KISG and its adjacent hosts. The FW configuration within the KISG requires an understanding of the network traffic routing principles, NAT technology operating concepts, firewall operation skills, and knowledge of the IDS and IPS.

This manual describes the specifics of the KISG firewall running in various KISG modes: NAT, routing, and modem. Detailed descriptions of these modes are given in the “Examples of the KISG firewall application for various implementation schemes” section. Handling of the IDS events will be discussed using a sample scenario of the FW rules configuration with the KISG running in the NAT mode. The specifics of data traffic routing in the KISG will be described by an example of configuration of FW rules in the routing mode. The use of configuration files to set up a wireless connection will be described by an example of configuring the KISG in the modem mode.

3 Description of the firewall operation

The KISG firewall monitors and filters the network traffic that passes through it according to its filtering rules. The KISG FW is built on the basis of the NPF (New Packet Filter), which is a firewall developed under the NetBSD project.

The rules added via the FW are compiled only for inbound connections for the LAN and WAN zones. In terms of the NPF, these rules are designated by the keyword “in”. For a user, it means that it is possible to create inbound rules for either WAN or LAN, but absolutely impossible to create outbound (“out”) rules for the KISG.

The specific of the KISG FW operation is that it runs in the stateful mode. Stateful firewalls are firewalls that track the complete state of the active network connections. Unlike stateless firewalls, stateful firewalls analyze the traffic taking into account communication parameters, which makes it possible to transfer the data back via the FW without the need to create an additional rule for response packets. In other words, stateful firewalls remember the connection initiator instead of separate traffic packets or data, which allows the response packets to go through the FW back to the source of the network connection.

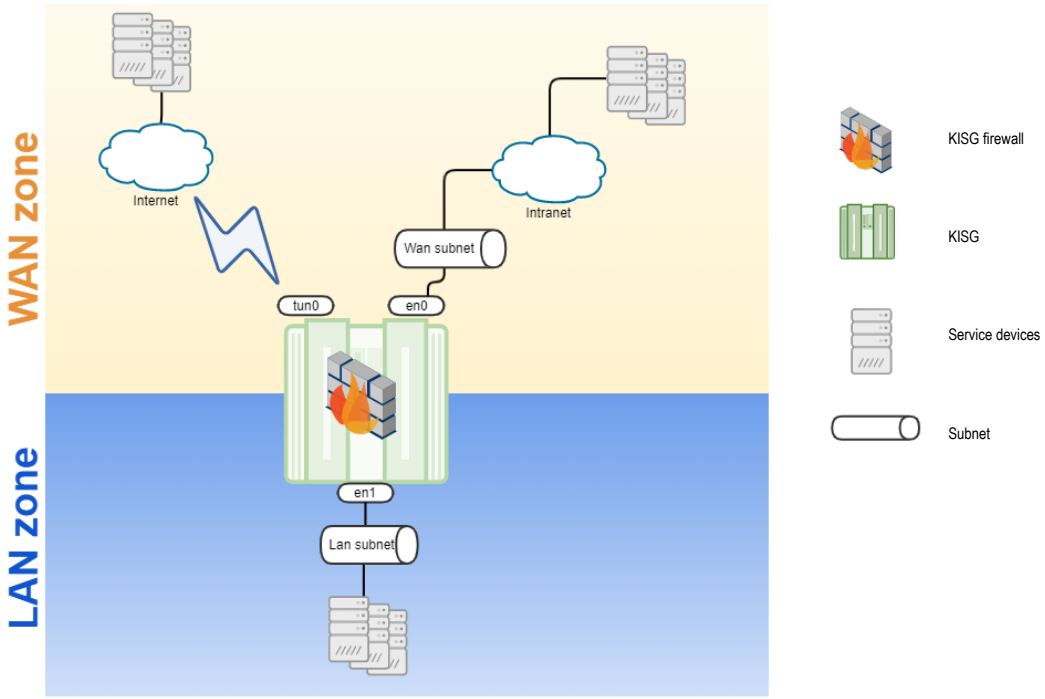
3.1 Description of network segments

The FW works with two network zones in the KISG with the following FW rules set between them:

- WAN (the tun0 wireless interface and the en0 Ethernet adapter).
- LAN (the en1 Ethernet adapter).

The tun0 is the interface of the wireless modem. The en0 and en1 interfaces are hard-wired Ethernet adapters on the sides of the WAN and LAN zones, respectively. The WAN zone includes the devices connected on the side of the WAN interface (en0 or tun0 modem), while the LAN zone includes devices connected on the side of the LAN interface (en1).

The figure below shows the layout diagram of the security zones with respect to the FW of the KISG. The LAN and WAN zones on the diagram are designated as “LAN zone” and “WAN zone”, respectively.



The FW rules are configured separately for the LAN and WAN zones.

3.2 FW rule sources

The set of the FW rules that determines traffic filtering is formed on the basis of the following rules and lists:

- As a result of applying the list of FW service rules (**SystemRules**), which by default always allows a connection to the KISG web-interface, interaction between the KISG, the Kaspersky Security Center (KSC), DHCP, and DNS, as well as with the Syslog server and MQTT devices.
- The list of trusted IP addresses (**AllowListRules**) of hosts which are ignored by the IDS.
- The list of blocked IP addresses (**BlockedListRules**), which is filled by the IPS component built into the KISG. The IPS component generates deny rules as a result of triggering the intrusion prevention system (IDS).
- Manually set FW rules (**UserFirewallRules**) configured with the KSC control plug-in.

The process of creating the FW rules is described in 3. Creation of Firewall Rules.

There are the following restrictions in the KISG firewall:

- Rules cannot be created using the DNS name of the allowed or blocked host.
- The IPS component works only from the side of the WAN.

3.3 Application of FW rules

3.3.1 Resultant FW rule policy

The resultant policy of FW rules is formed on the basis of manually and automatically set rules as well as FW service rules.

The FW rules are applied in the following order:

1) SystemRules, allow rules for the service protocols;

2) AllowListRules, exception rules to be checked by the IDS component;

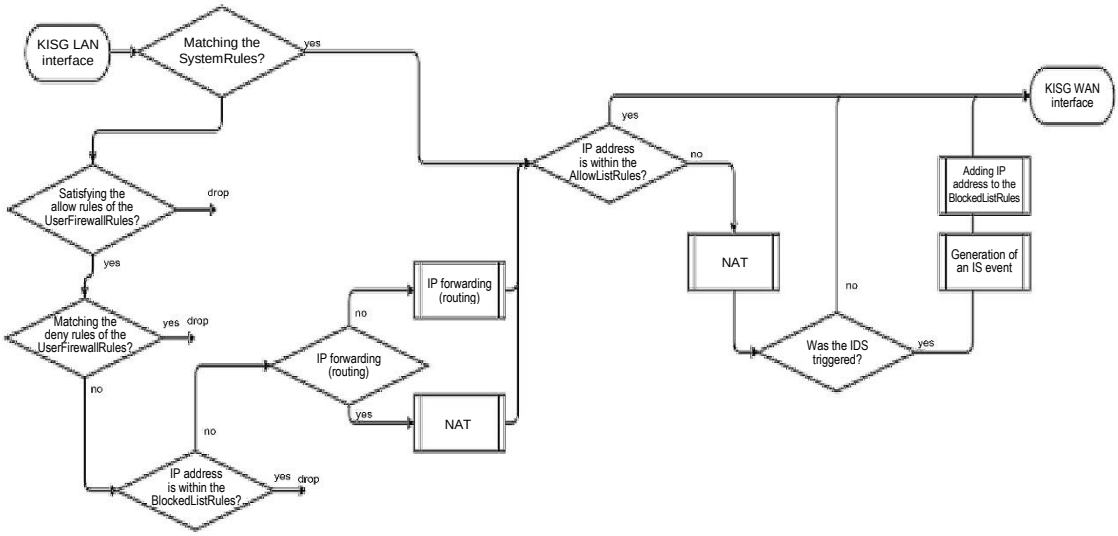
3) BlockedListRules, rules including the list of blocked IP addresses generated by the IPS (i.e. it is filled after the IDS is triggered);

4) UserFirewallRules, manually set FW rules for the LAN and WAN zones;

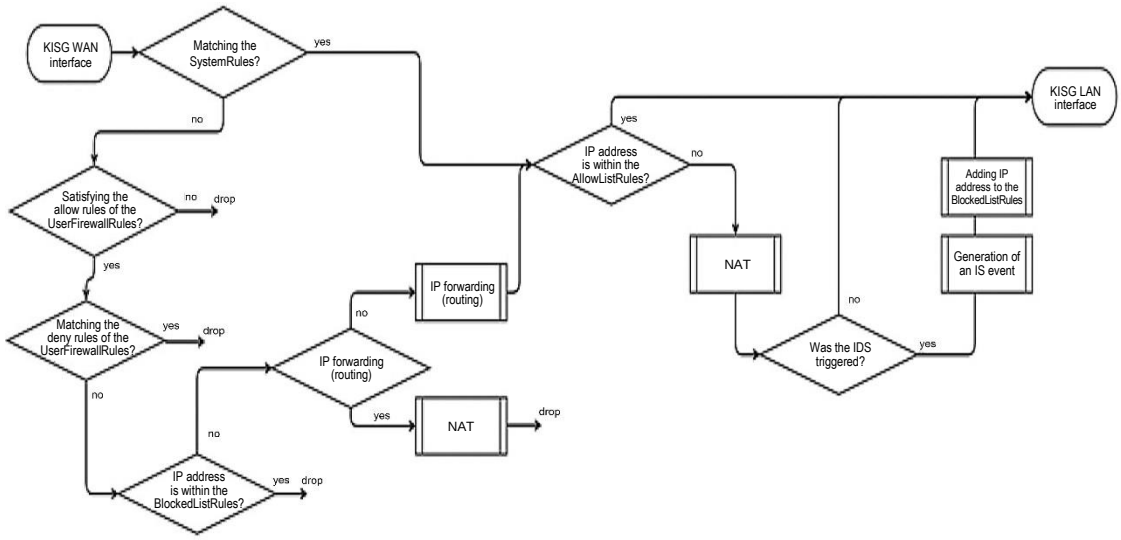
5) default deny rules “default deny any:any → any:any”.

All rules are final. In other words, if a coincidence with some rule occurs, then the other rules of this list will not be considered for the packet after this. The figure below shows the application schemes for the KISG firewall rules used for packet transfer between the LAN and the WAN zones in both directions, represented by packet flow diagrams.

FW rule application when a packet is transferred from the LAN to the WAN zone



FW rule application when a packet is transferred from the WAN to the LAN zone



At the WAN interface, the rules are marked as stateful irrespective of the selected protocol, whether it is UDP or TCP.

3.3.2 Current service rules of access to the MQTT, KSC, and Syslog (SystemRules)

Some rules are formed because of the setup of the KISG parameters; therefore, the description of the FW rules will need some designations for the following parameters:

- **IPv4_LAN_KISG** is the IP address of LAN interface of the KISG.
- **IPv4_WAN_KISG** is the IP address of active WAN interface of the KISG (tun0 or en0).
- **IPv4_KSC_SERVER** is the IP address of the KSC server specified within the KISG settings.
- **IPv4_SYSLOG_SERVER** is the IP address of the Syslog server, specified within the KISG settings.
- **PORT_SYSLOG_SERVER** is the port intended to receive connections of the Syslog server, specified within the KISG settings.
- **IPv4_MQTT_CLOUD_BROKER** is the IP address of the MQTT broker within the cloud from the side of the WAN zone.
- **IPv4_UPDATE_SERVER** is the web server where the KISG update file is located.
- **PORT_UPDATE_SERVER** is the TCP port for connection to the web host where the KISG update file is located.

Symbol "→" indicates the traffic direction from which the connection is initiated.

By default, there is a deny rule set in the KISG for all interactions (see the table below).

Protocol: Brief description	Action	Zone / L4 protocol / IP address: Source port number → IP address :Target port number
Default deny rule	Deny	- WAN / any / any:any → any:any; - LAN / any / any:any → any:any

The allow service rules SystemRules work over the deny rules (see the table below).

Protocol: Brief description	Action	Zone / L4 protocol / IP address: Source port number → IP address :Target port number

Service protocol for communication with the KSC server	Allow	- WAN / TCP / any:any → <IPv4_KSC_SERVER>:13294; - LAN / TCP / any:any → <IPv4_KSC_SERVER>:13294
HTTPS: Web interface of KISG control	Allow	- LAN / TCP / any:any → <IP address of the KISG>:443;
UDP, TCP, TCP/TLS: Transmission of messages to the Syslog server	Allow	- WAN / UDP / any:any → <IPv4_SYSLOG_SERVER>:514; - WAN / TCP / any:any → <IPv4_SYSLOG_SERVER>:514; - WAN / TCP / any:any → <IPv4_SYSLOG_SERVER>:<PORT_SYSLOG_SERVER>;
MQTT: Re-transmission of MQTT messages to the cloud	Allow	- WAN / tcp / <IPv4_WAN_KISG>:any → <IPv4_MQTT_CLOUD_BROKER>:8883; - LAN / tcp / <IPv4_LAN_KISG>:any → <IPv4_MQTT_CLOUD_BROKER>:8883;
MQTT: Receiving MQTT messages from devices within the LAN zone	Allow	- LAN / tcp / any:any → <IPv4_LAN_KISG>:1883; - LAN / udp / any:any → <IPv4_LAN_KISG>:1883;
DNS: DNS requests	Allow	- WAN / udp / <IPv4_WAN_KISG>:any → any:53; - LAN / udp / any:any → any:53;
DNS: DNS responses	Allow	- WAN / udp / any:53 → any:any;
DHCP: Sending a request to the WAN zone for the KISG interface IP address via DHCP	Allow	- WAN / udp / any:68 → any:67;
DHCP: Receiving a response to a request to the WAN zone for the KISG interface IP address via DHCP	Allow	- WAN / udp / any:67 → any:68;
DHCP: Receiving requests for IP addresses for devices within the LAN zone via DHCP	Allow	- LAN / udp / any:68 → <IPv4_LAN_KISG>:67;
DHCP: Sending a response to a request for the IP address for devices within the LAN zone via DHCP	Allow	- LAN / udp / <IPv4_LAN_KISG>:67 → any:68;
Receiving an update to the KISG	Allow	- WAN / tcp / <IPv4_WAN_KISG>:any → <IPv4_UPDATE_SERVER>:<PORT_UPDATE_SERVER>;

If necessary, the user can create their own firewalling rules. Manually added rules are called the UserFirewallRules. The process of creating FW user rules is described in the online KISG help in Section 3. Creation of Firewall Rules.

4 Specifics of the IDS/IPS operation

4.1 Function of the IDS component within the KISG

The IDS component of the KISG helps to identify basic malicious networking. During the IDS activity, considering the security purposes (8. Security Purposes and Assumptions), it is assumed that:

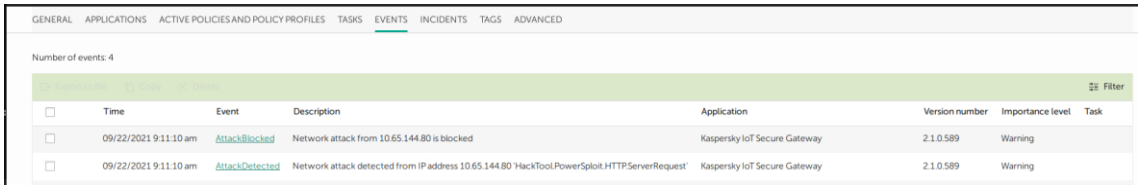
- By default, all traffic is forbidden when the KISG starts. This traffic is subject to the SystemRules deny rules to avoid unauthorized networking.
- The threat sources from the WAN side are treated as medium-level threats (basic higher level).
- The threat sources from the LAN side are treated as low-level threats (basic level).

Based on the KISG security assumptions (see 8. Security Purposes and Assumptions), the device that has the Kaspersky IoT Secure Gateway installed works in an environment that guarantees no physical access of an intruder, including access for a direct connection to the device. Namely, the probability of an unauthorized connection from the side of the LAN zone is lower than that from the side of the WAN zone. There are intruders from both the LAN and the WAN sides, but approaches to protection from each of these intruder categories are different. The KISG uses both the IDS/IPS and the FW for protection from intruders within the WAN zone, but only the latter for protection from intruders within the LAN zone.

However, the IDS triggering events may occur for hosts within the LAN zone as well. In the routing mode, attack detection and host blocking for the LAN zone are exactly as for the WAN zone. However, if the KISG is running in the NAT mode, the IDS/IPS will be able to block attacks from hosts within the WAN zone only because the packet comes to the IDS component with a substituted IP address and port number after the NAT. The IDS can also trigger for IP addresses of hosts from the LAN zone, but in this situation, the IP address of the WAN interface will be indicated as an attack source. The address of the WAN interface is not on the BlockedListRules list since it is on the SystemRules allow rules list. If the source of malicious networking is detected from the side of the WAN zone, then such an address will be added to BlockedListRules.

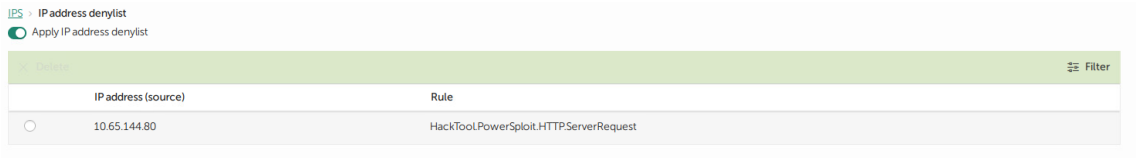
4.2 Analysis of IDS/IPS events

When the IDS is triggered, an IDS triggering event is formed and a host blocking message appears. A message including the incident description and the name of the triggered IDS signature will appear in the KISG web interface. This message will be transferred to the KSC as well as to the Syslog server, to the Google (FCM) push notifications server, or to the MQTT broker. The IP address of the host that is the source of malicious networking is added to the list of the blocked IP addresses (BlockedListRules). An example of such a message can be seen after synchronization with the KSC. In the KSC plug-in, you will get a message about the detection of malicious networking and the blocking of the attacking host.

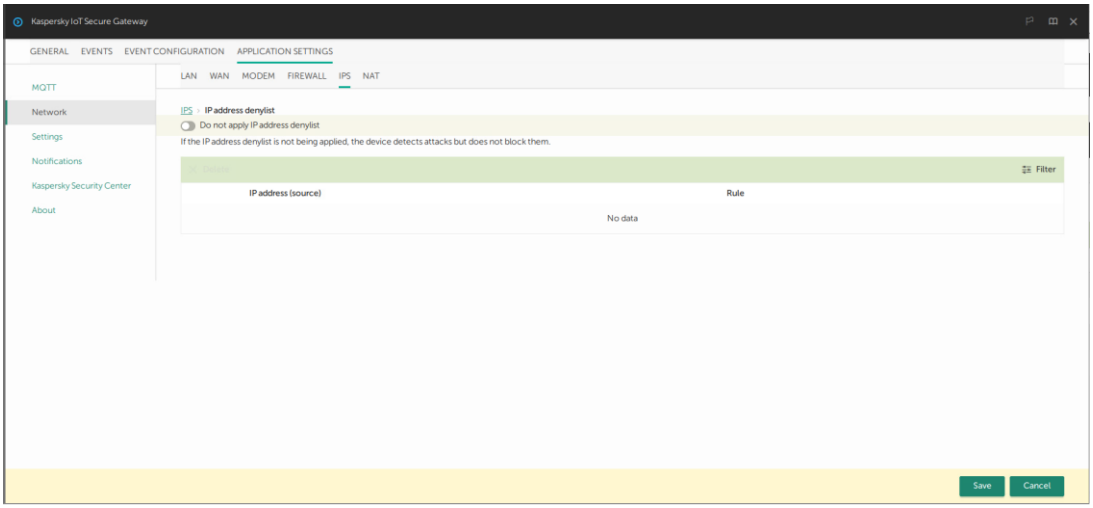


4.3 Work with blocked IP addresses. The BlockedListRules list and adding exceptions to the AllowListRules list for the IDS

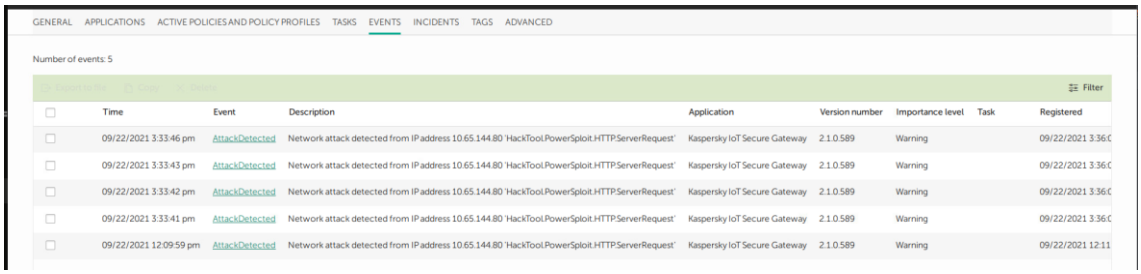
After the IDS is triggered, the IP address of the malicious host is added to the BlockedListRules list. The device can be unblocked by checking the box across from the IP address of the blocked host and clicking the Delete button. After the KISG is synchronized with the KSC, the host will be unblocked.



If the “Apply IP address deny list” toggle switch is on, attack detection events will be generated after an IDS incident, but the malicious hosts will not be blocked.
4. Switching the Forbidden IP Address List On and Off



After the “Apply IP address deny list” toggle switch is turned off, you will not receive messages about the blocking of hosts when IDS triggering events occur.



To avoid IDS triggering for a certain host, add its IP address to the AllowListRules list. 2. Adding an IP Address to the Allowed IP Address List

If the IP address is added to the AllowListRules list, the IDS will not check connections for this host.

4.4 Improvement of detection quality

It is not recommended to add a rule with the format “allow any:any→ any:any” for the LAN and WAN interface to the FW. This will reduce the protection level of the security zones, since it will allow a potentially malicious networking, and the IDS/IPS component will possibly have to track more network connections through the KISG. Setting precise FW rules reduces the IDS load and the amount of the potentially false triggering events.

5 Examples of the KISG firewall application for various implementation schemes

When configuring the FW in the KISG, it is necessary to consider its mode.

The main KISG modes are:

- NAT with NAT enabled in the KISG.
- Routing with NAT enabled in the mode of packet routing between the LAN and WAN (hereinafter referred to as the routing mode).
- Modem with the modem enabled.

The process of switching between the NAT and routing modes is described in Section 7. Masquerading Setup. The process of configuring the wireless connection is addressed in Section 5. Setting up Wireless Connection.

Below are the instructions on the FW configuration in each of these modes.

5.1 Preparation for access control

The following actions are required before configuring the FW rules:

1. Log in to the KISG using the web-interface. 1. Scenario: Quick Start for Admin
2. Configure the communication with the KSC. 4. Setting Up the Connection with the Kaspersky Security Center

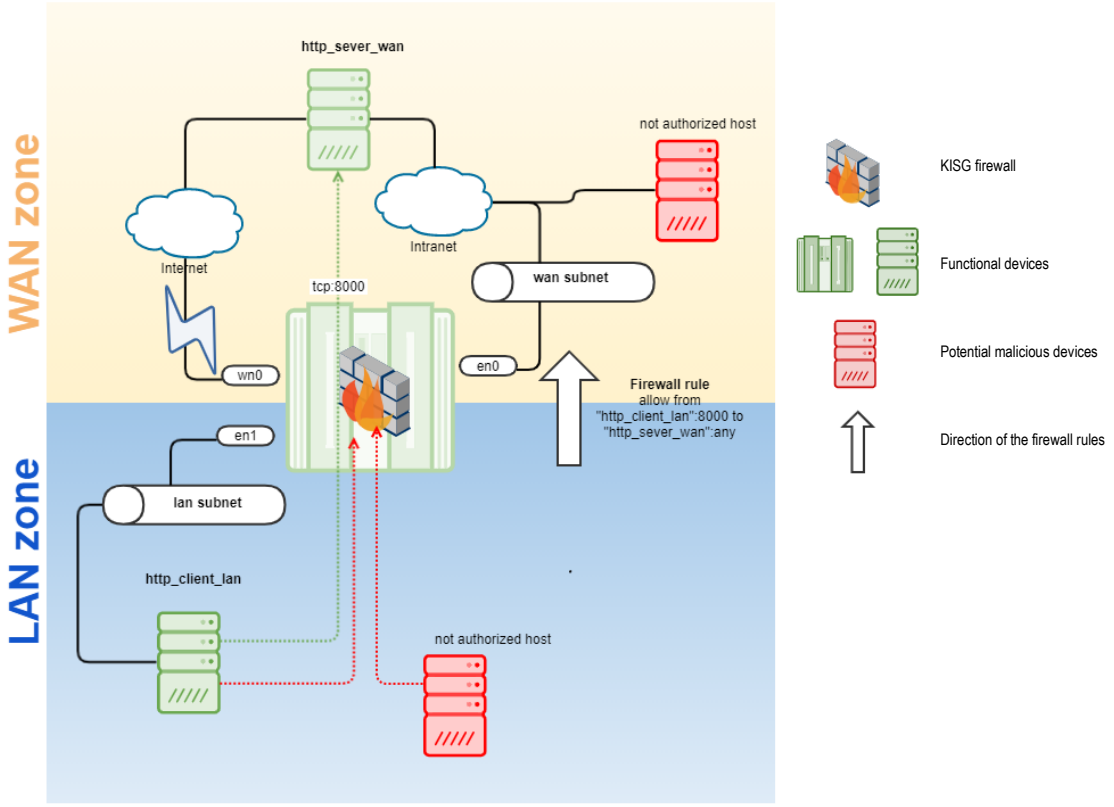
After this, it is possible to configure the FW rules in the KSC web console interface. 3. Creation of Firewall Rules.

5.2 Implementation scheme with NAT enabled in the KISG

In this mode, the KISG performs SNAT (Source Network Address Translation), which is essentially a mechanism substituting the source address during packet forwarding. The initial IP address of a source within the LAN zone is transformed into an IP address of the WAN interface of the KISG with the source port being substituted. For response packets, an inverse transformation of the IP address and the target port takes place. SNAT prevents external sources from directly accessing the server instances. Thus, a host from the WAN zone cannot initialize a connection to the hosts of the LAN zone.

The KISG has tun0 and en0 interfaces within the WAN zone. The en0 interface is hardwired, while the tun0 interface is the modem interface. Only one of these interfaces can be active at a given time, and if masquerading is switched on, the NAT turns on at the active interface only. Thus, if the modem is the main link, then the KISG will perform SNAT between the en1 and the tun0. At this moment, the WAN interface en0 will not run. If the wireless connection is not active, then en0 will be the active interface.

The diagram below illustrates the position of various devices with respect to the KISG.



Located in the WAN zone segment are all devices connected to the KISG interface with the modem tun0 and to the KISG Ethernet adapter en0. The WAN zone is highlighted in orange.

Located in the LAN zone segment are the devices connected to the KISG Ethernet adapter en1. The LAN zone security zone is highlighted in blue.

The WAN interface must be configured in such a way that the DNS server, the KSC server, and the MQTT broker are accessible within the cloud. The DNS server must be able to allow the KSC name specified in the certificate which was added in the KISG web interface. If the certificate for connection to the KSC is issued for an IP address, then it is not necessary to set up the DNS server. You can read more details on the process of adding a certificate in section 4. Setting Up the Connection with the Kaspersky Security Center.

If the main link is switched to the modem, the FW can be configured similarly to the situation when the KISG is running in the NAT mode. Namely, the allow rule of the UserFirewallRules should also be added for the LAN zone. This KISG application scheme will be discussed in Section 6.3.

5.2.1 Access control for a host from the LAN zone with the KISG running in the NAT mode

When the KISG is running in the NAT mode, in order to control access from the LAN zone, it is sufficient to add the allow rule of the UserFirewallRules for the LAN zone only, while it's not necessary to create such a rule for the WAN zone. This is because the IP address of the connection source is substituted when a packet is transferred via the KISG. The packet comes to the WAN zone with the substituted IP address and port. For the response packet, the IP address and the connection source port are substituted.

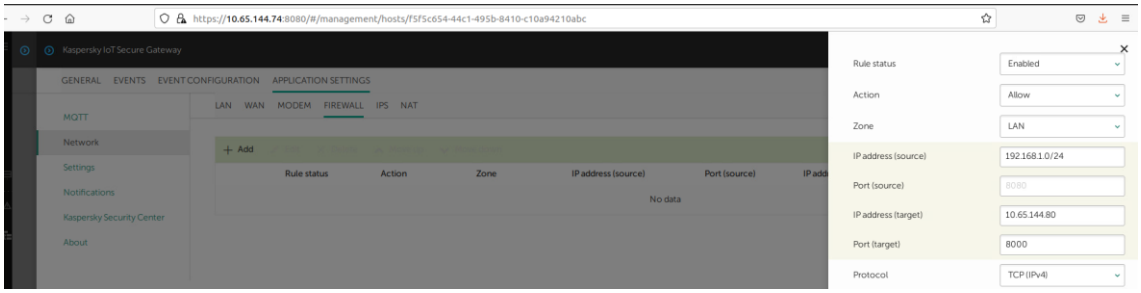
For example, let us consider a scenario where it is necessary to configure HTTP access from a host within the LAN zone to a host in the WAN zone.

If the field is left empty, then the value ANY will be applied. It is possible to specify both an IP address (e.g. 192.168.4.5) and subnet (e.g. 192.168.8.0/24) in the fields “IP address (source)” and “IP address (target)”.

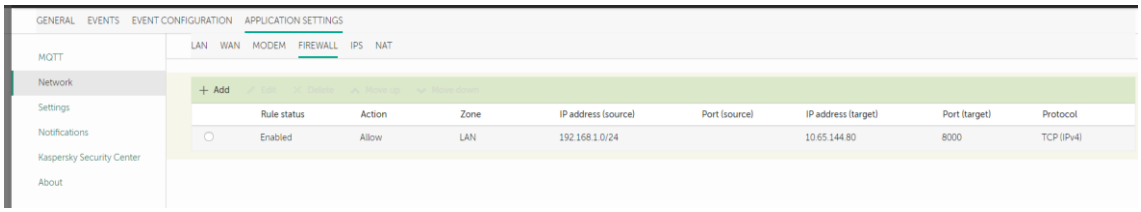
Let us assume that the IP address of the host “http_client_lan” is 192.168.1.20, while the IP address of the host “http_server_wan” is 10.65.144.80. Thus, the following FW rule should be added:

Action	Zone / L4 protocol / IP address: Source port number → IP address :Target port number
Allow	- LAN / TCP / 192.168.1.0/24:any → 10.65.144.80:8000

Therefore, within the interface of the KSC plug-in, the allow rule for tcp:8000 will look as follows:



After you click the OK button, the new rule will appear within the created rule list:



Click Save and close the KISG properties window.

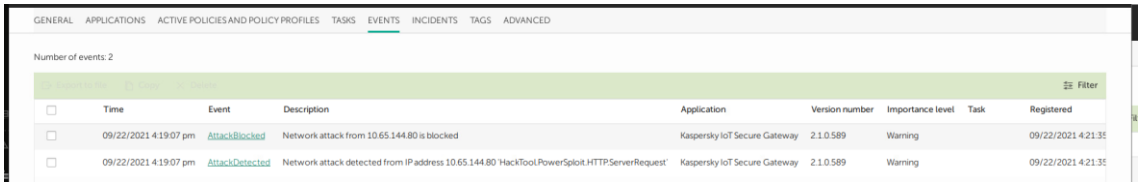
After the rule is applied, you have to wait for the KISG and KSC to be synchronized. You can learn the time of synchronization by closing the KISG properties window. It will be displayed in the column “Last connection to Administrator center”.

After the synchronization, the host “http_client_lan” can connect to the host “http_server_wan”.

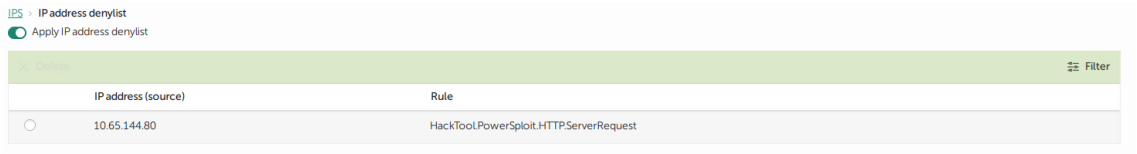
5.2.2 Blocking a host after an IDS event

If there are no IDS incidents, the host “http_client_lan” can get access to the host “http_server_wan” via port 8000.

If the KISG detects malicious traffic, the IP address of the host that is the source of malicious activity will be added to the BlockedListRules list and blocked. In the KISG web interface, you will get a message about the IDS being triggered and about the blocking of host 10.65.144.80:



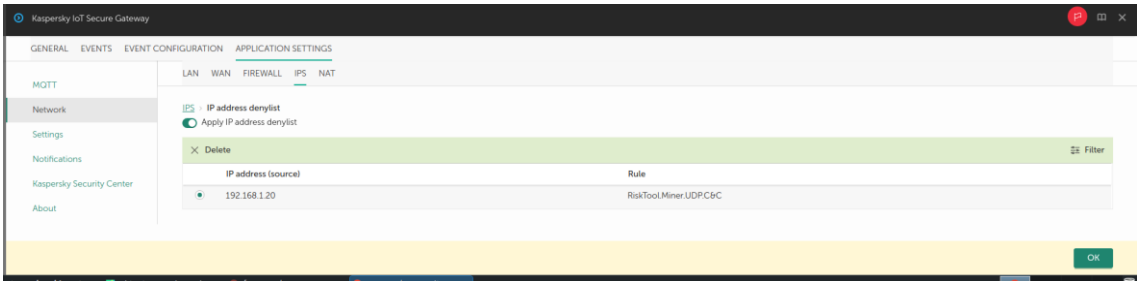
The host with the IP address of the attack source will appear on the BlockedListRules list.



Network connections between the host “http_server_wan” and the host with the IP address 10.65.144.80 will be blocked by the KISG-based FW.

Below you will find the ways to unblock a device which have been added on the BlockedListRules list:

- Wait 60 minutes: when 60 minutes have passed, the IP address of the blocked device will be removed from the BlockedListRules list.
- Manually remove the “http_server_wan” host’s IP address from the BlockedListRules list. 3. Removing an IP address from the Allowed IP Address List



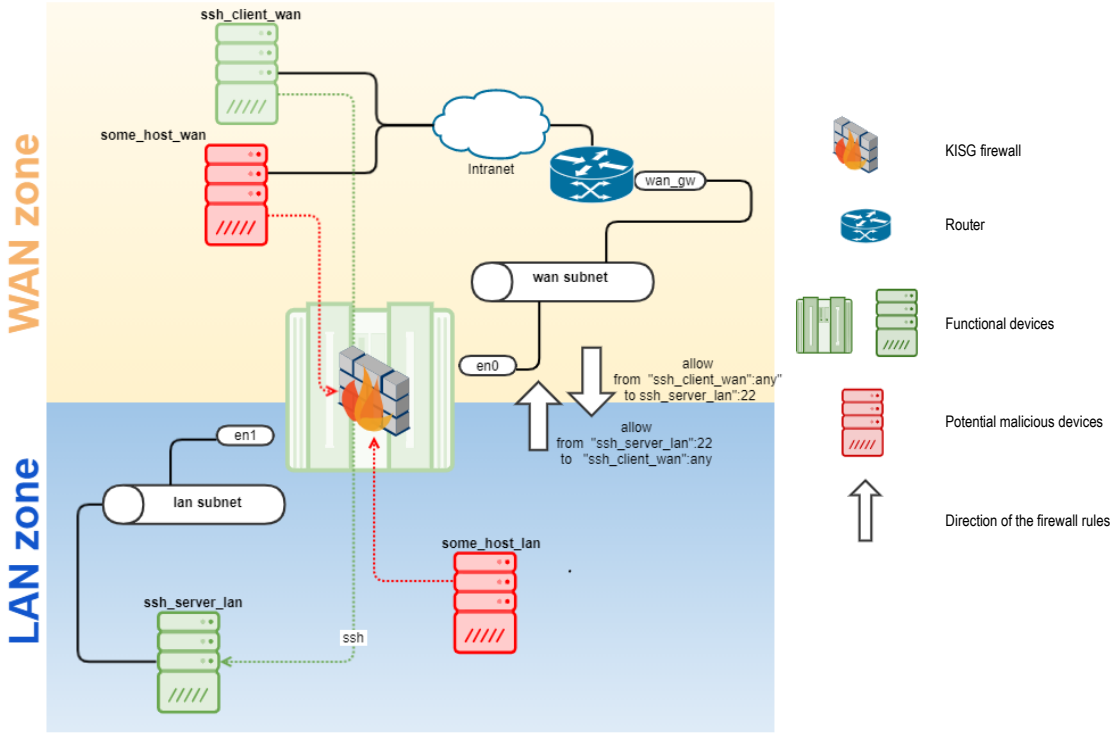
5.3 Implementation scheme with the KISG running in the packet routing mode

Details on the access configuration from the WAN zone to the LAN zone are given in Section 2. Scenario: Configuring Access from an External Network to the Devices of an Internal Network.

Below you will find an example of controlling the SSH access of the host “ssh_client_wan” to the host “ssh_server_lan”. Access control can be divided into 2 steps:

1) setting up routing and checking the network accessibility;

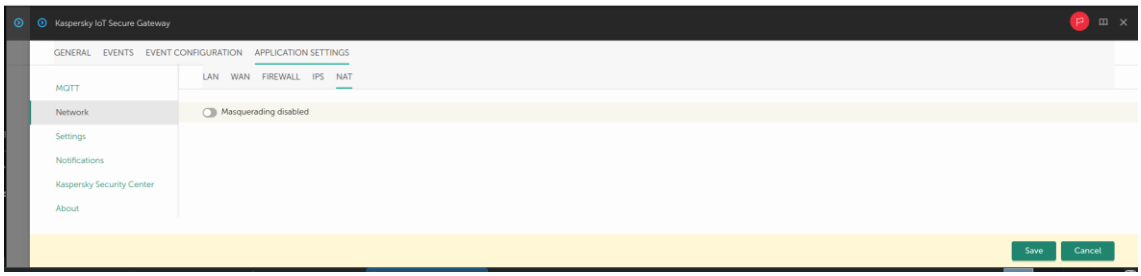
2) adding the FW rules for the LAN and WAN zones.



Let us consider each of these steps in more detail.

5.3.1 Routing

For packet routing from the WAN to the LAN by the KISG, it is necessary to disable the NAT mode using the KSC plug-in. In order to do this within the KSC web interface, go to the controlled KISG properties, select the “Application settings” tab, “Network”, then select “NAT” and toggle the switch:



For details on switching, refer to 7. Masquerading Setup.

Then it is necessary to verify the correctness of the routing setup at the network devices that are working together with the KISG. This is especially necessary for the router within the WAN zone that routes traffic to the intranet.

The following paths should be set up at the router:

- Path from the intranet to the LAN subnet (lan subnet) with the IP address of the WAN interface of the KISG (en0) as a gateway.
- Path from the LAN subnet (lan subnet) to the intranet segment with the router interface (wan_gw) as a gateway.

To avoid path loss at the router, it is recommended to set a static IP address at the WAN interface of the KISG (en0). To set a static IP address, follow the instructions on 2. Setting Up External Network Parameters. If the WAN interface of the KISG receives an IP address via

DHCP, then routing to the LAN subnet will fail when the IP address of the WAN interface changes. It will be necessary to update the router's routing rules.

The actual IP addresses and paths for the KISG can be found within the KSC web interface at https://192.168.1.1/troubleshooting.

If routing is set up correctly, then the host "ssh_client_wan" should be able to ping the host "ssh_server_lan". The KISG firewall does not block the ICMP packets.

Before connecting the KISG to the router, it is desirable to ensure that the WAN subnet (wan subnet) at the router differs from the LAN subnet (lan subnet). Many routers often work with subnet 192.168.1.0/24, like the LAN interface of the KISG.

5.3.2 Access control for a host from the WAN zone with the KISG running in the routing mode

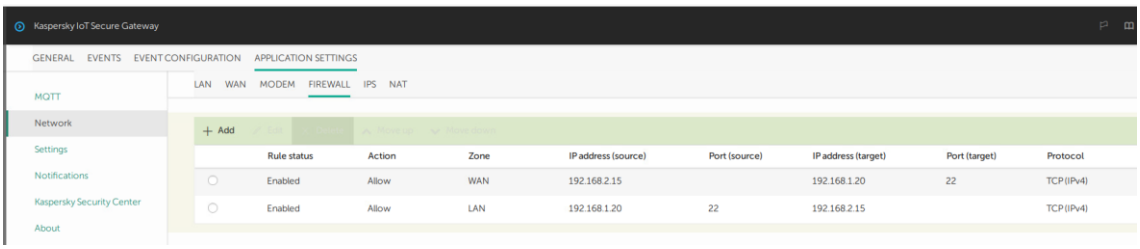
Unlike the situation with the KISG running in the NAT mode, the rule should be added not only for the LAN zone but for the WAN zone as well.

Let us assume that the IP address of the host "ssh_client_wan" is 192.168.2.15, while the IP address of the host "ssh_server_lan" is 192.168.1.20. It is assumed that the devices within the LAN zone receive IP addresses via DHCP. In such a situation, a subnet 192.168.1.0/24 rather than the particular address 192.168.1.20 should be specified. At least the following FW rules should then be set up in the KISG:

Action	Zone / L4 protocol / IP address: Source port number → IP address :Target port number
Allow	- LAN / TCP / 192.168.1.0/24:22 → 192.168.2.15:any
Allow	- WAN / TCP / 192.168.2.15:any → 192.168.1.0/24:22

In this case, it is sufficient to add two rules. The rule "WAN / TCP / 192.168.2.15:any → 192.168.1.0/24:22" is an inbound stateful rule at the WAN interface of the KISG. The rule "LAN / TCP / 192.168.1.0/24:22 → 192.168.2.15:any" plays the role of an inbound stateless rule for the LAN zone. The stateless rule must be added when controlling access from the WAN zone to the LAN zone due to the architecture of FW implementation in the KISG.

The final list of FW rules will look like this in the KSC console:

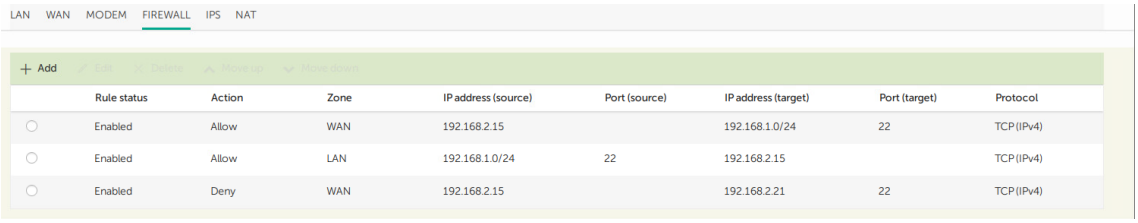


After adding the rules from the WAN zone to the LAN zone, it might be required to reload the KISG to apply them.

5.3.3 Adding a deny rule for a host from the WAN zone with the KISG running in the routing mode

If a host in the WAN zone needs to restrict access to the LAN zone, you must add a deny rule along with the allow rules:

Action	Zone / L4 protocol / IP address: Source port number → IP address :Target port number
Allow	- LAN / TCP / 192.168.1.0/24:22 → 192.168.2.15:any
Allow	- WAN / TCP / 192.168.2.15:any → 192.168.1.0/24:22
Deny	- WAN / TCP / 192.168.2.15:any → 192.168.1.21:22



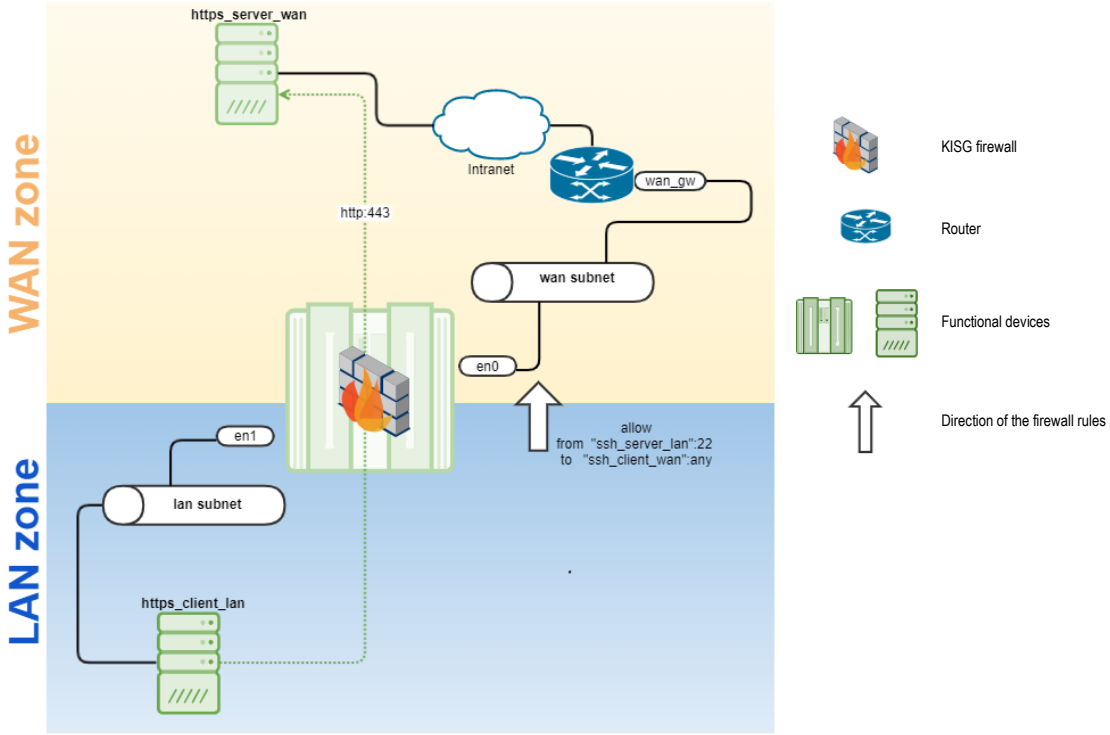
	Rule status	Action	Zone	IP address (source)	Port (source)	IP address (target)	Port (target)	Protocol
○	Enabled	Allow	WAN	192.168.2.15		192.168.1.0/24	22	TCP (IPv4)
○	Enabled	Allow	LAN	192.168.1.0/24	22	192.168.2.15		TCP (IPv4)
○	Enabled	Deny	WAN	192.168.2.15		192.168.2.21	22	TCP (IPv4)

After the settings are synchronized between the KSC and the KISG, the host “ssh_client_wan” will not be able to connect to the host “ssh_server_lan”.

After applying this rule, it may be necessary to reload the KISG.

5.3.4 Access control for a host from the LAN zone with the KISG running in the routing mode

In the routing mode, control of access from the LAN zone to the WAN zone does not differ from the access control approach in the NAT mode.



Let us assume that the IP address of the host “https_client_lan” is 192.168.1.20, while the IP address of the host “https_server_wan” is 10.65.144.80. If it is necessary to control the “https_client_wan” host’s access to the host “https_server_wan” via port 443, then the FW rule will look like this:

Action	Zone / L4 protocol / IP address: Source port number → IP address :Target port number
Allow	- LAN / TCP / 192.168.1.20:any → 10.65.144.80:443

5.4 KISG configuration in the modem mode

IMPORTANT!

- The SIM card installed in the UTX-3117 should support operation via a modem. You can clarify the SIM card data plan and switch it to the modem mode by contacting your service provider.
- To allow a device within the LAN zone to get Internet access via the KISG modem, the host within the LAN zone should obtain the network settings from the DHCP server of the KISG.

You must configure the wireless connection profile in order to work with the modem. By default, the KISG has preset profiles for communications providers MTS, Beeline, and Megafon. You can select an existing profile from the preset list (for providers MTS, Beeline, and Megafon) or create a new profile (3. Creating a New Modem Profile). A new profile is required if the provider's settings differ from the standard ones.

When the profile has been created, it is necessary to activate the desired profile (1. Table of Modem Profiles), restart the KISG, and turn on the wireless data transfer mode 2. Turning a Wireless Connection On and Off.

The examples of the PPP configuration files for MTS, Beeline, and Megafon can be found in the KISG web interface. These configuration files are ready for setting up a wireless connection with a mobile network operator via a modem.

More details on the functioning of the PPP protocol are available at:

http://www.bsdportal.ru/fdocs/books/handbook/userppp.html

Examples of the PPP configuration files are available at:

https://github.com/FreeBSDDesktop/freebsd-base/tree/master/share/examples/ppp

6 Identification of a matching implementation scheme

Selecting the KISG implementation scheme, you should consider the following factors depending on the mode:

NAT	Routing
Remember that rules can only be created based on IP addresses	Remember that rules can only be created based on IP addresses
When a packet is transferred from the LAN zone to the WAN zone via the KISG, the IP address is substituted	To access the LAN, you must specify a path to the LAN subnet via the WAN interface of the KISG at the router within the WAN zone; in this situation, it is better to set a static routing at the KISG
Access from the WAN zone to the LAN zone is impossible	The FW rules should be set for both the LAN and WAN zones
It is sufficient to set the FW rules for the LAN zone	

The diagram below illustrates the possible data traffic. This diagram will help you understand which hosts you will need to create FW rules for and which hosts will run without manually set FW rules. The devices highlighted with green and blue have had service rules applied. The deny rule “default deny any:any->any:any” has been applied to the grey and red devices.