Документирование работы FW для KISG

1. Условные обозначения

KISG – Kaspersky IoT Secure Gateway;

IDS – intrusion detection system (система обнаружения сетевых вторжений);

IPS – intrusion prevention system (система предотвращения сетевых вторжений);

LAN – наименование внутренней зоны относительно KISG;

WAN – наименование внешней зоны относительно KISG;

МСЭ – межсетевой экран (или firewall);

ИБ – информационная безопасность.

NAT – Network Address Translation (преобразование сетевых адресов);

KSC – сервер Kaspersky Security Center

SSH - Secure Shell (сетевой протокол прикладного уровня, позволяющий производить защищенное удалённое управление);

HTTP - HyperText Transfer Protocol (протокол прикладного уровня для передачи данных);

MQTT - message queuing telemetry transport (упрощённый сетевой протокол, работающий поверх TCP/IP, ориентированный на обмен сообщениями между устройствами по принципу издатель-подписчик);

PPP - Point-to-Point Protocol (двухточечный протокол канального уровня).

2. Введение

Данное руководство знакомит специалистов, внедряющих Kaspersky IoT Secure Gateway (далее KISG), с особенностями настройки Межсетевого экрана (далее МСЭ) в зависимости от схемы внедрения KISG. В руководстве приведены инструкции по следующим процедурам:

- настройка сетевой доступности для хостов, находящихся в различных сегментах KISG;

- анализ событий информационной безопасности;
- корректировка правил межсетевого экранирования.

Межсетевой экран в KISG предназначен для фильтрации запрещенного трафика. МСЭ с жестко настроенными правилами блокирует излишние сетевые соединения, что снижает вероятность возникновения потенциального вредоносного сетевого взаимодействия через KISG, а IDS/IPS позволяет обнаруживать базовые сетевые атаки на KISG и смежные хосты. Для настройки межсетевого экрана в KISG необходимо понимание принципов маршрутизации сетевого трафика, принципов работы технологии NAT, навыки работы с межсетевыми экранами, а также представление об IDS и IPS.

В руководстве описаны особенности работы межсетевого экрана KISG в различных режимах функционирования KISG: "NAT", "routing" и "modem" подробное описание режимов работы приведено в разделе "Примеры применения межсетевого экрана KISG при различных схемах внедрения" . На примере сценария по настройке МСЭ-правил в режиме работы KISG в режиме "NAT" будет рассмотрена работа с событиями IDS. На примере по настройке МСЭ-правил в режиме "routing" будут рассмотрены особенности маршрутизации информационных потоков в KISG. На примере настройки KISG в режиме "modem" будет описан процесс применения конфигурационных файлов для настройки беспроводного соединения.

3. Описание работы межсетевого экрана

Межсетевой экран KISG осуществляет контроль и фильтрацию проходящего через него сетевого трафика в соответствии с правилами фильтрации. МСЭ KISG построен на базе NPF (New Packet Filter) — межсетевого экрана, разработанного в рамках проекта NetBSD.

Правила, добавленные через МСЭ, компилируются только для входящих соединений для LAN- и WAN-зон. В терминологии NPF это правила, которые обозначаются ключевым словом "in". Для пользователя это означает, что он может сделать входящие правила для WAN, либо для LAN, но никак не исходящие (out) от KISG правила.

Особенностью работы межсетевого экрана в KISG является то, что межсетевой экран KISG работает в режиме "stateful". Межсетевые экраны с отслеживанием состояния (далее stateful firewall)- это межсетевые экраны, которые отслеживают полное состояние активных сетевых подключений. В отличии от межсетевых экранов без сохранения состояния активных сетевых подключений (stateless firewall) "stateful firewall" анализируют трафик с учетом параметров соединения. Это позволяет передавать обратно данные через МСЭ без необходимости создавать дополнительное правило для ответных пакетов. Иными словами, "stateful firewall" запоминают инициатора соединения, а не отдельные пакеты трафика и данных, что позволяет ответным пакетам проходить через МСЭ обратно к источнику сетевого соединения.

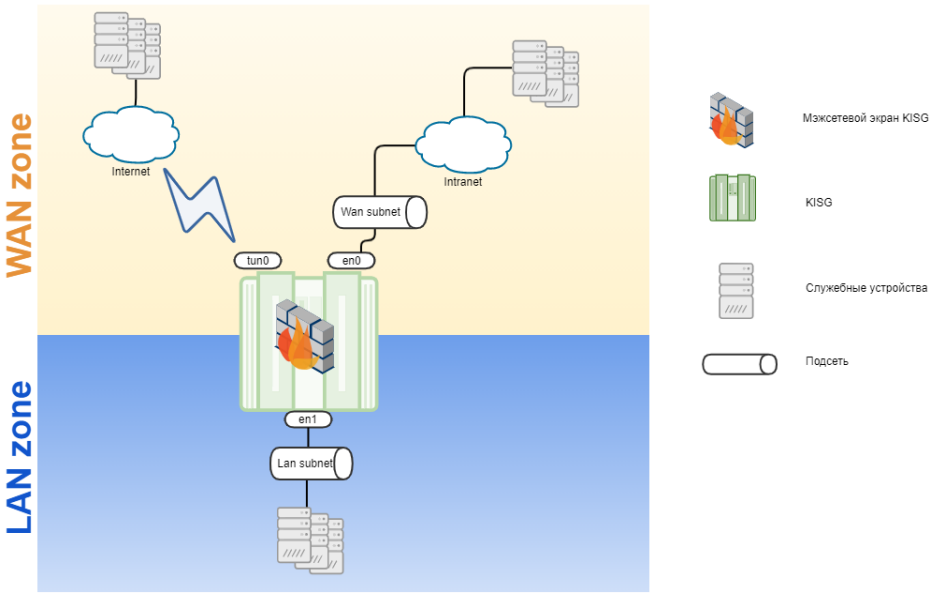
3.1. Описание сетевых сегментов

МСЭ в KISG работает с двумя сетевыми зонами, межу которыми настраиваются правила МСЭ:

- WAN (беспроводной интерфейс "tun0" и eth-адептер "en0");
- LAN (eth-адептер "en1").

Интерфейс "tun0" - это интерфейс беспроводного модема. Интерфейсы "en0" и "en1" - проводные ethernet-адаптеры со стороны WAN-зоны и LAN-зоны соответственно. В WAN-зону входят устройства, подключенные со стороны WAN-интерфейса ("en0" или модема "tun0"), а в LAN-зону входят устройства, подключенные со стороны LAN-интерфейса ("en1").

На рисунке ниже приведена схема расположения зон безопасности относительно межсетевого экрана в KISG. На схеме LAN- и WAN-зона будут о бозначены как "LAN zone" и "WAN zone" соответственно.



Для LAN-зоны и WAN-зоны правила МСЭ настраиваются отдельно.

3.2. Источники правил МСЭ

Комплекс правил межсетевого экрана, определяющий фильтрацию трафика, формируется, исходя из следующих правил и списков:

- в результате действия списка служебных правил МСЭ (**SystemRules**), которые по умолчанию всегда разрешают подключение к web-интерфейсу KISG, взаимодействие между KISG и Kaspersky Security Center (далее KSC), DHCP, DNS, с сервером Syslog и с MQTT-устройствами;
- списка доверенных IP-адресов (**AllowListRules**) хостов, которые IDS игнорирует;
- списка заблокированных IP-адресов (**BlockedListRules**), который наполняется с помощью встроенного в KISG компонента IPS. Компонент IPS формирует запрещающие правила в результате срабатывания системы предотвращения сетевых вторжений (далее IDS);
- ручных правил МСЭ (**UserFirewallRules**), настраиваемых с помощью плагина управления KSC.

Процесс создания правил межсетевого экрана описан в статье: 3. Создание правил межсетевого экрана.

Существуют следующие ограничения для межсетевого экрана KISG:

- Отсутствует возможность создания правила по DNS-имени разрешаемого или блокируемого хоста.
- IPS-компонент работает только со стороны WAN.

3.3. Порядок применения правил МСЭ

3.3.1. Результирующая политика правил МСЭ

Результирующая политика МСЭ формируется на основе ручных, автоматических и служебных правил МСЭ.

Правила межсетевого экрана применяются в следующем порядке:

1) SystemRules – разрешающие правила для служебных протоколов;

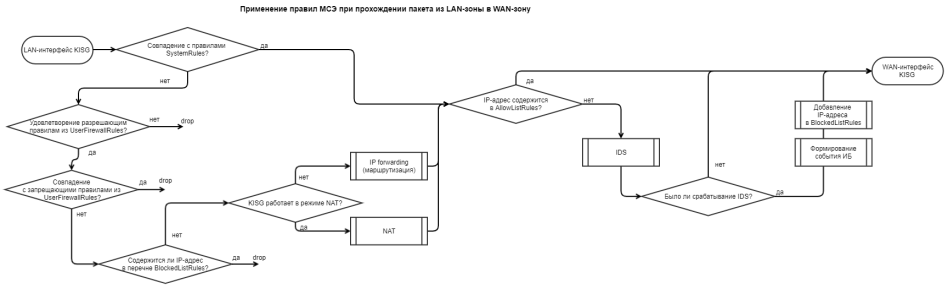
2) AllowListRules – правила для исключений проверки компонентом IDS;

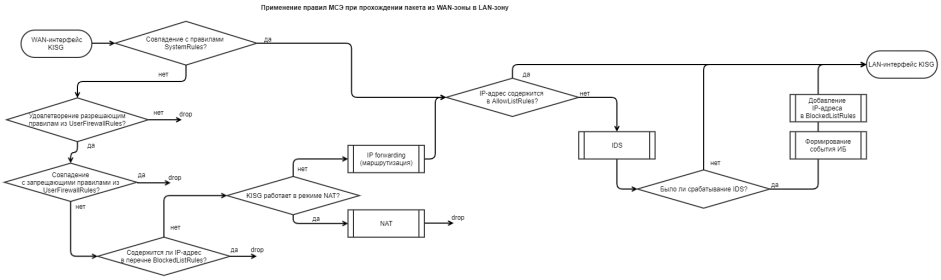
3) BlockedListRules – правила, включающие в себя перечень заблокированных IP-адресов. Формируется за счет IPS(т.е. наполняется после срабатывания IDS);

4) UserFirewallRules – ручные правила МСЭ для LAN- и WAN-зоны;

5) Запрещающие правила по умолчанию "default deny any:any → any:any".

Все правила являются финальными. Иными словами, если произошло совпадение с каким либо правилом, то дальше другие правила из этого списка или перечня для пакета рассматриваться не будут. На рисунке ниже представлены схемы применения правил межсетевого экрана KISG при прохождении пакета из LAN-зоны в WAN-зону и при прохождении из WAN-зоны в LAN-зону в виде "packet flow"-диаграмм.





Правила на WAN интерфейсе помечаются как stateful вне зависимости от выбранного протокола: будь до UDP или TCP.

3.3.2. Действующие служебные правила для доступа к MQTT, KSC, Syslog (SystemRules)

Часть правил формируется в результате настройки параметров KISG, поэтому для описания правил МСЭ потребуются некоторые условные обозначения для следующих параметров:

- **IPv4_LAN_KISG** – IP-адрес LAN-интерфейса KISG;
- **IPv4_WAN_KISG** – IP-адрес активного WAN-интерфейса KISG ("tun0" или "en0");
- **IPv4_KSC_SERVER** – IP-адрес KSC-сервера, указанный в настройках KISG;
- **IPv4_SYSLOG_SERVER** – IP-адрес Syslog-сервера, указанный в настройках KISG;
- **PORT_SYSLOG_SERVER** – порт для приема соединений Syslog-сервера, указанный в настройках KISG;
- **IPv4_MQTT_CLOUD_BROKER**– IP-адрес MQTT-брокера в облаке со стороны WAN-зоны;
- **IPv4_UPDATE_SERVER** – web-сервер, на котором размещается файл обновлений KISG;
- **PORT_UPDATE_SERVER** – tcp-порт для подключения к web-хосту, на котором размещается файл обновлений KISG.

Символ "→" указывает направление трафика, откуда производится инициализация соединения.

По умолчанию в KISG выставлено запрещающее правило для всех взаимодействий (см. таблицу ниже).

Протокол: Краткое описание	Действие	Зона / Протокол L4 / IP-адрес: Номер порта источника → IP-адрес :Номер порта назначения
Запрещающее правило по умолчанию	Запретить	- WAN / any / any:any → any:any; - LAN / any / any:any → any:any

Поверх запрещающих правил работают разрешающие служебные правила "SystemRules" (см. таблицу ниже):

Протокол: Краткое описание	Действие	Зона / Протокол L4 / IP-адрес: Номер порта источника → IP-адрес :Номер порта назначения
Служебный протокол для связи с KSC-сервером	Разрешить	- WAN / TCP / any:any → <IPv4_KSC_SERVER>:13294; - LAN / TCP / any:any → <IPv4_KSC_SERVER>:13294

HTTPS: Web-интерфейс управления KISG	Разрешить	- LAN / TCP / any:any → <IP-адрес KISG>:443;
UDP, TCP, TCP/TLS: Передача сообщений на Syslog-сервер	Разрешить	- 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: Пересылка MQTT-сообщений в облако	Разрешить	- WAN / tcp / <IPv4_WAN_KISG>: any → <IPv4_MQTT_CLOUD_BROKER>:8883; - LAN / tcp / <IPv4_LAN_KISG>: any → <IPv4_MQTT_CLOUD_BROKER>:8883;
MQTT: Прием MQTT-сообщений от устройств в LAN-зоне	Разрешить	- LAN / tcp / any:any → <IPv4_LAN_KISG>:1883; - LAN / udp / any:any → <IPv4_LAN_KISG>:1883;
DNS: DNS-запросы	Разрешить	- WAN / udp / <IPv4_WAN_KISG>:any → any:53; - LAN / udp / any:any → any:53;
DNS: DNS-ответы	Разрешить	- WAN / udp / any:53 → any:any;
DHCP: Отправка запроса на получение ip-адреса по DHCP для интерфейса KISG WAN-зоне	Разрешить	- WAN / udp / any:68 → any:67;
DHCP: Получение ответа на запрос ip-адреса по DHCP для интерфейса KISG WAN-зоне	Разрешить	- WAN / udp / any:67 → any:68;
DHCP: Прием запросов на выдачу ip-адресов по DHCP для устройств в LAN-зоне	Разрешить	- LAN / udp / any:68 → <IPv4_LAN_KISG>:67;
DHCP: Отправка ответа на запрос ip-адреса по DHCP для устройств в LAN-зоне	Разрешить	- LAN / udp / <IPv4_LAN_KISG>:67 → any:68;
Получение обновления KISG	Разрешить	- WAN / tcp / <IPv4_WAN_KISG>:any → <IPv4_UPDATE_SERVER>:<PORT_UPDATE_SERVER>;

При необходимости можно самостоятельно создавать правила межсетевого экранирования. Правила, добавленные вручную, называются пользовательскими правилами - "UserFirewallRules". Процесс создания пользовательских правил межсетевого экрана описан в онлайн-справке KISG в разделе 3. Создание правил межсетевого экрана

4. Особенности работы IDS/IPS

4.1. Назначение компонента IDS в KISG

Компонент IDS KISG позволяет обнаруживать базовые сетевые вредоносные взаимодействия. При работе IDS KISG, учитывая цели безопасности (8. Цели и предположения безопасности.), предполагается, что:

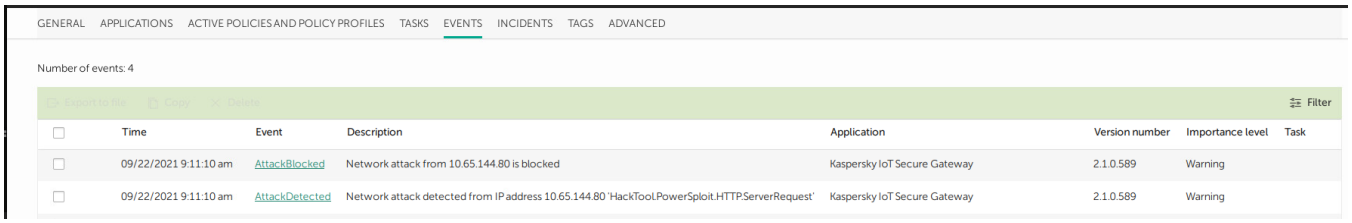
- По умолчанию при старте KISG запрещен весь трафик. Этот трафик попадает под действие правил запрещающих правил "SystemRules" для исключения несанкционированного сетевого взаимодействия;
- Источники угроз со стороны WAN сети имеют средний уровень угроз (базовый повышенный);
- Источники угроз со стороны LAN сети имеют низкий уровень угроз (базовый);

Исходя из предположений безопасности KISG (которые описаны в 8. Цели и предположения безопасности.), устройство, на котором установлен Kaspersky IoT Secure Gateway, работает в окружении, гарантирующем отсутствие физического доступа со стороны злоумышленника, в том числе для подключения напрямую к устройству. Т.е. со стороны LAN-зоны вероятность несанкционированного подключения ниже, чем со стороны WAN-зоны. Злоумышленники есть как со стороны LAN, так и со стороны WAN, но подходы к защите от каждой из категорий злоумышленников отличаются. От злоумышленников в WAN-зоне KISG защищается как с помощью IDS/IPS, так и с помощью МСЭ, а от злоумышленников в LAN сети с помощью МСЭ.

Однако срабатывания IDS могут быть и для хостов в LAN-зоне. В режиме работы "routing" обнаружение атак и блокировка хостов для LAN-зоны производится точно также как и для WAN-зоны. Но если KISG работает в режиме "NAT", то IDS/IPS сможет заблокировать атаки только от хостов в WAN-зоне. Это объясняется тем, что пакет приходит на IDS-компонент с подмененным IP-адресом и портом после NAT. На IP-адреса хостов из LAN-зоны также могут быть срабатывания IDS, но в таком случае в качестве источника атаки будет указан IP-адрес WAN-интерфейса. Адрес WAN-интерфейса не попадает в "BlockedListRules", т.к. он содержится в списке разрешающих правил "SystemRules". Если источник вредоносного взаимодействия будет определен со стороны WAN-зоны, то такой адрес добавится в "BlockedListRules".

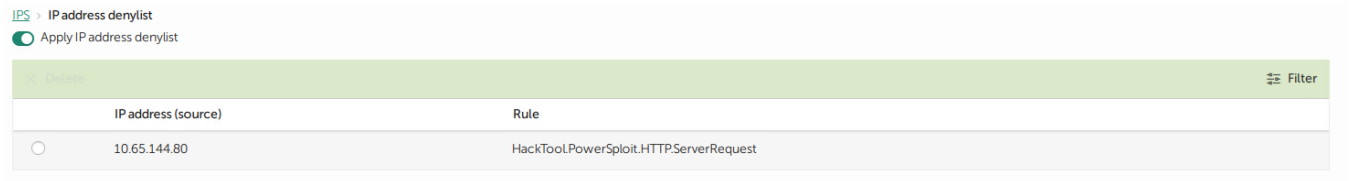
4.2. Анализ событий IDS/IPS

При срабатывании IDS формируется событие о срабатывании IDS и сообщение о блокировке хоста. В в web-интерфейсе KISG появится сообщение, которое будет содержать описание инцидента и имя сработавшей IDS-сигнатуры. Сообщение будет передано в KSC, а также на Syslog-сервер, сервер push-уведомлений Google (FCM) или на MQTT-брокер. IP-адрес хоста-источника вредоносного воздействия добавляется в перечень заблокированных IP-адресов (BlockedListRules). Пример такого сообщения можно наблюдать после синхронизации с KSC в plugin KSC появится сообщение об обнаружении вредоносного взаимодействия и о блокировке атакующего хоста.



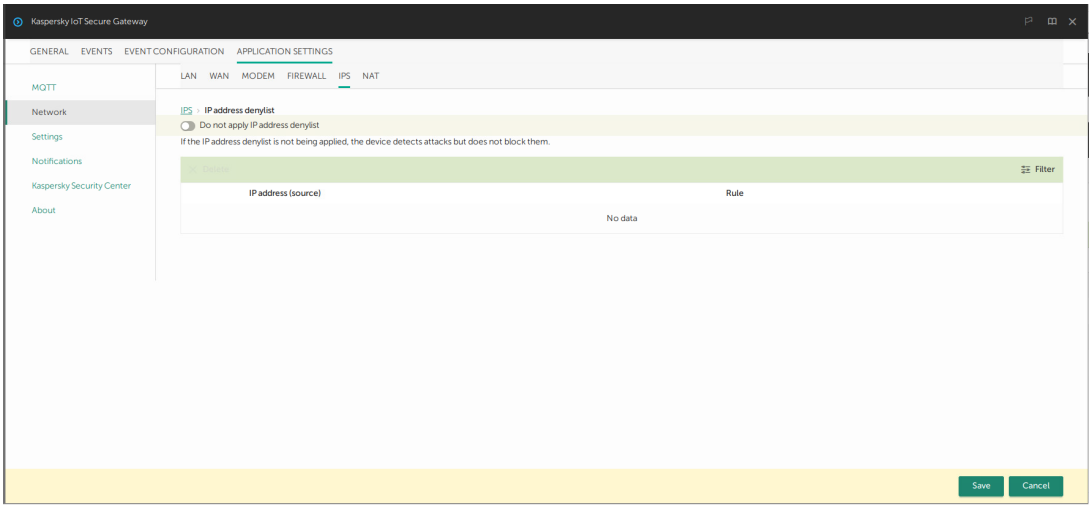
4.3. Работа с заблокированными IP-адресами "BlockedListRules" и добавление исключений для IDS "AllowListRules"

После срабатывания IDS IP-адрес вредоносного хоста попадает в "BlockedListRules". Разблокировать устройство можно, нажав чекбокс напротив IP-адреса заблокированного хоста и кнопку "Delete". После синхронизации KISG с KSC хост разблокируется.

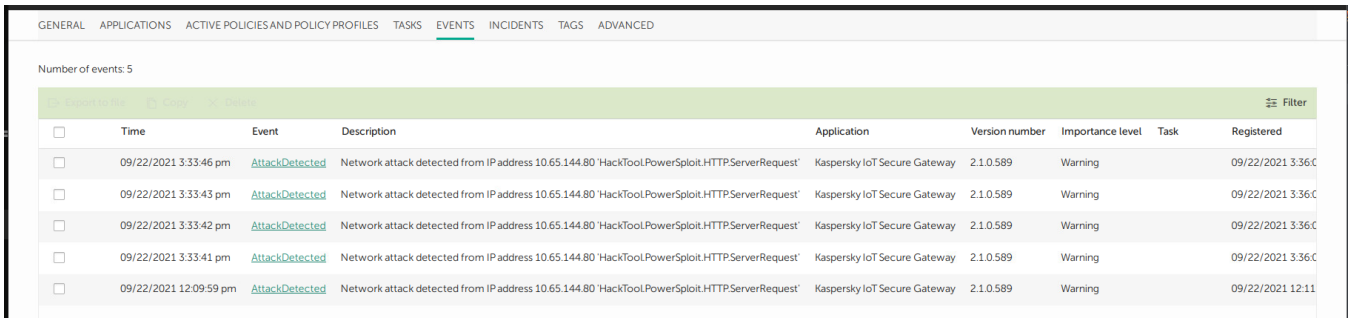


Если выключить тумблер "Apply IP address deny list", то после возникновения IDS инцидента будут формироваться события об обнаружении атаки, но вредоносные хосты блокироваться не будут.

4. Включение и выключение списка запрещенных IP-адресов



Таким образом после выключения тублера "Apply IP address deny list" при срабатывании событий IDS собщения о блокировке хоста появляться не будут.



Чтобы исключить срабатывания IDS для какого либо хоста, необходимо добавить IP-адрес хоста в "AllowListRules". 2. Добавление IP-адреса в список разрешенных IP-адресов

Если IP-адрес добавлен в "AllowListRules", то IDS не будет производить проверку соединений для этого хоста.

4.4. Улучшение качества детектирования

Не стоит добавлять в МСЭ правила формата "allow any:any→ any:any" для интерфейса LAN и WAN, Это снизит уровень защищенности зон безопасности, т.к. таким образом будут разрешены потенциально вредоносные сетевые взаимодействия, а компоненту IDS/IPS возможно придется следить за большим количеством сетевых соединений, проходящих через KISG. Настройка точных правил МСЭ снижает нагрузку на IDS и уменьшает количество потенциально возможных ложных срабатываний.

5. Примеры применения межсетевого экрана KISG при различных схемах внедрения

В процессе настройки МСЭ в KISG необходимо учитывать режим его режим работы.

Основные режимы работы KISG:

- NAT – с включенным NAT на KISG;
- routing – с выключенным NAT в режиме маршрутизации пакетов между LAN и WAN (далее в режиме маршрутизации);
- modem – с включенным модемом.

Процесс переключения между режимом "NAT" или "routing" описан в разделе 7. Настройка маскарадинга. Процесс настройки беспроводного соединения описан в разделе 5. Настройка параметров беспроводного соединения.

Ниже приведены указания по настройке МСЭ в каждом из режимов работы.

5.1. Подготовка к разграничению доступа

Перед настройкой правил МСЭ нужно выполнить следующие действия:

1. Необходимо авторизоваться в KISG, используя веб-интерфейс. 1. Сценарий: Быстрый старт для администратора;
2. Настроить связь с KSC 4. Настройка параметров подключения к Kaspersky Security Center;

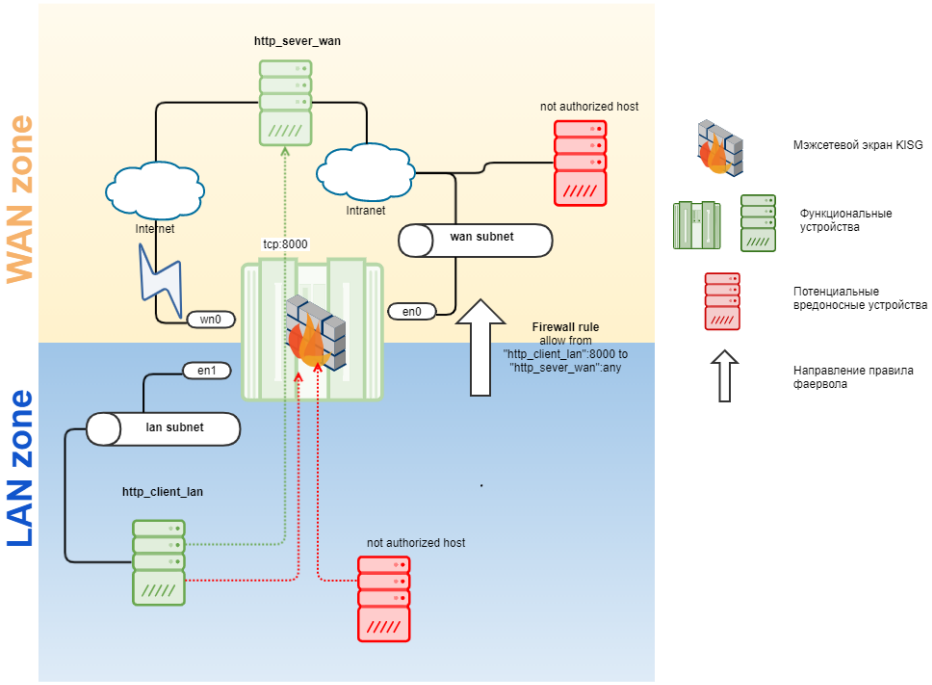
После этого в интерфейсе веб-консоли KSC можно настраивать правила МСЭ 3. Создание правил межсетевого экрана.

5.2. Описание схемы внедрения при включенном NAT на KISG

В таком режиме работы KISG осуществляет SNAT (Source Network Address Translation) – механизм, суть которого состоит в замене адреса источника при пересылке пакета. Исходный IP-адрес источника, расположенного в LAN-зоне преобразуется в IP-адрес WAN-интерфейса KISG с заменой порта источника. Для ответных пакетов производится обратное преобразование для IP-адреса и порта назначения. SNAT не позволяет внешним источникам напрямую обращаться к серверным экземплярам. Т.е. хост из WAN-зоны не может инициализировать соединения к хостам LAN-зоне.

В WAN-зоне у KISG расположены интерфейсы "tun0" и "en0". Интерфейс "en0" является проводным, а интерфейс "tun0" является интерфейсом модема. Активным может быть только один этих интерфейсов, и при включении маскарадинга NAT включается только активном интерфейсе. Т. е. если основным каналом является модем, то KISG будет осуществлять SNAT между "en1" и "tun0". В этот момент времени WAN-интерфейс "en0" работать не будет. Если беспроводное соединение будет неактивно, то активным интерфейсом будет "en0".

Ниже приведена иллюстрация схемы расположения различных устройств относительно KISG:



В сегменте "WAN zone" находятся все устройства, подключенные к интерфейсу KISG с модемом "tun0" и Ethernet-адаптеру KISG "en0". На рисунке "WAN zone" подсвечена оранжевым цветом.

В сегменте "LAN zone" находятся устройства, подключенные к Ethernet-адаптеру KISG "en1". Зона безопасности "LAN zone" выделена синим паттерном .

WAN-интерфейс необходимо сконфигурировать таким образом, чтобы были доступны DNS-сервер, сервер KSC и MQTT-брокера в облаке. Серве р DNS должен иметь возможность разрешать имя KSC, указанное в сертификате, который был добавлен в web-интерфейсе KISG. Если сертификат для подключения к KSC выписан на IP-адрес, то DNS-сервер настраивать не обязательно. Подробнее про процесс добавления сертификата можно почитать в разделе: 4. Настройка параметров подключения к Kaspersky Security Center.

Если переключить основной канал связи на модем, то МСЭ можно настроить по аналогии с режимом работы KISG в режиме "NAT". Т.е. разрешающее правило "UserFirewallRules" также надо добавить для LAN-зоны. Такая схема применения KISG будет рассмотрена в разделе "6.3".

5.2.1. Разграничение доступа для хоста из LAN-зоны при работе KISG в режиме работы NAT

При работе KISG в режиме NAT, чтобы разграничить доступ из LAN-зоны, достаточно добавить разрешающее правило "UserFirewallRules" только для LAN-зоны, а создавать разрешающее правило UserFirewallRules для WAN-зоны не нужно. Это объясняется тем, что происходит подмена IP-адреса источника соединения при прохождении пакета через KISG. В WAN-зону пакет попадает с замененными IP-адресом и портом. Для ответного пакета подставляются IP-адрес и порт источника соединения.

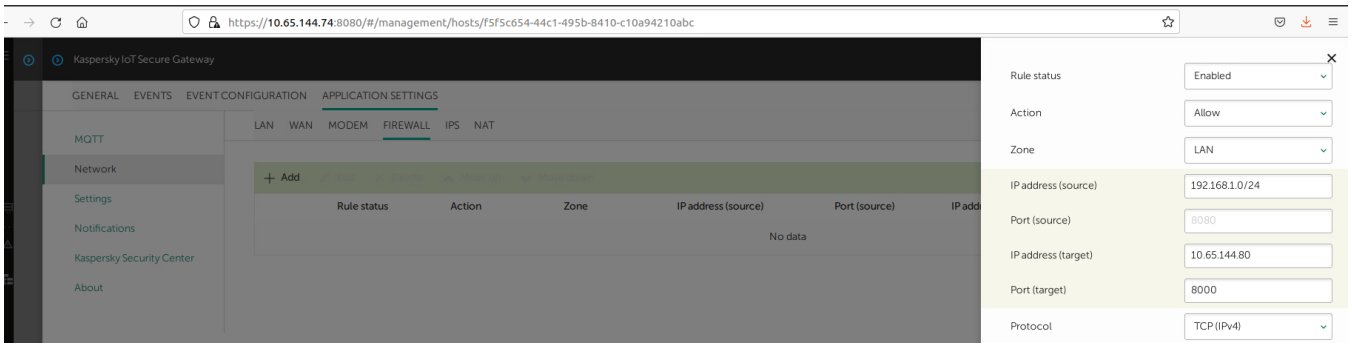
Для примера рассмотрим сценарий, когда для хоста из LAN-зоны необходимо настроить доступ к хосту в WAN-зоне по протоколу HTTP.

Если оставить поле незаполненным, то применится значение "ANY". В полях IP-адресов (source) и IP-адресов (target) можно указывать как IP-адрес (например, 192.168.4.5), так и подсеть (например, 192.168.8.0/24) .

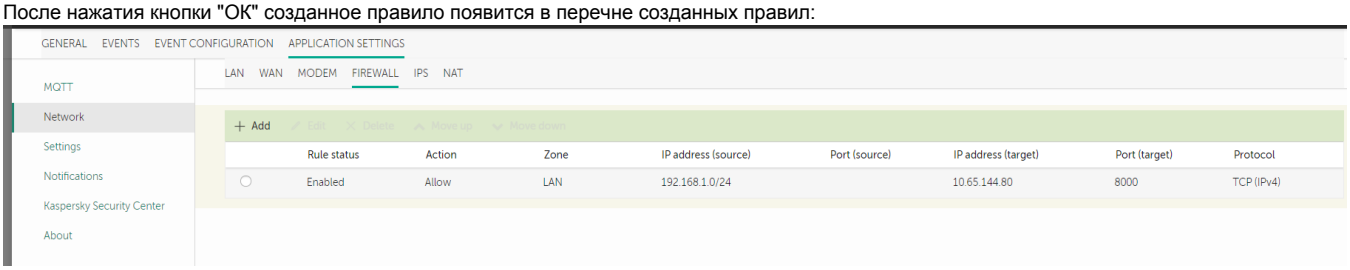
Допустим у хоста "http_client_lan" ip- адрес 192.168.1.20, а хоста "http_server_wan" ip-адрес 10.65.144.80. Таким образом нужно добавить следующее правило МСЭ:

Действие	Зона / Протокол L4 / IP-адрес: Номер порта источника → IP-адрес :Номер порта назначения
Разрешить	- LAN / TCP / 192.168.1.0/24:any → 10.65.144.80:8000

Таким образом в интерфейсе plugin KSC разрешающее правило для tcp:8000 будет выглядеть следующим образом:



После нажатия кнопки "ОК" созданное правило появится в перечне созданных правил:



Нажимаем "Save" и закрываем окно с свойствами KISG.

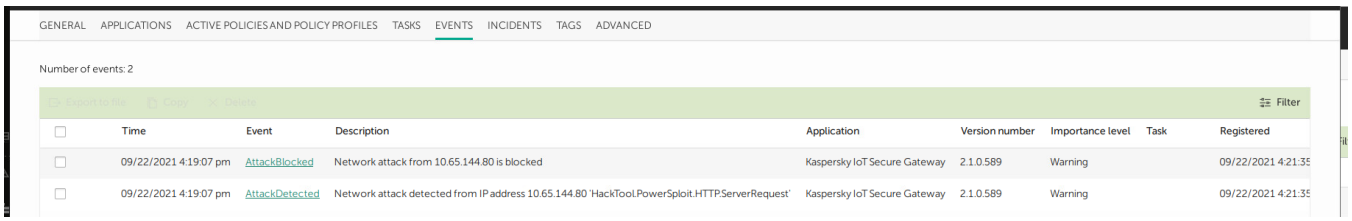
После применения правила необходимо дождаться синхронизации KISG и KSC. Узнать время синхронизации можно, закрыв окно со свойствами KISG. В столбце "Last connection to Administrator center" отобразится время синхронизации :

После синхронизации хост "http_client_lan" сможет выполнить подключение к "http_server_wan" .

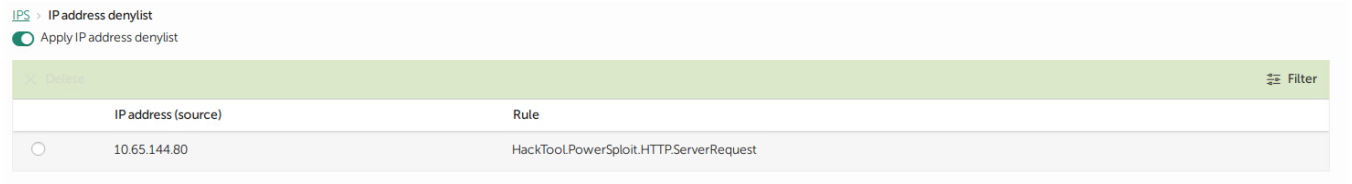
5.2.2. Блокировка хоста после IDS события

Без IDS-инцидентов "http_client_lan" может получать доступ к "http_server_wan" по порту 8000.

Если KISG зафиксирует вредоносный трафик, то IP-адрес хоста, с которого осуществляется вредоносная активность, будет добавлен в "BlockedListRules" и заблокирован. В web-интерфейсе KISG появится сообщение об срабатывании IDS и о блокировке хоста 10.65.144.80:



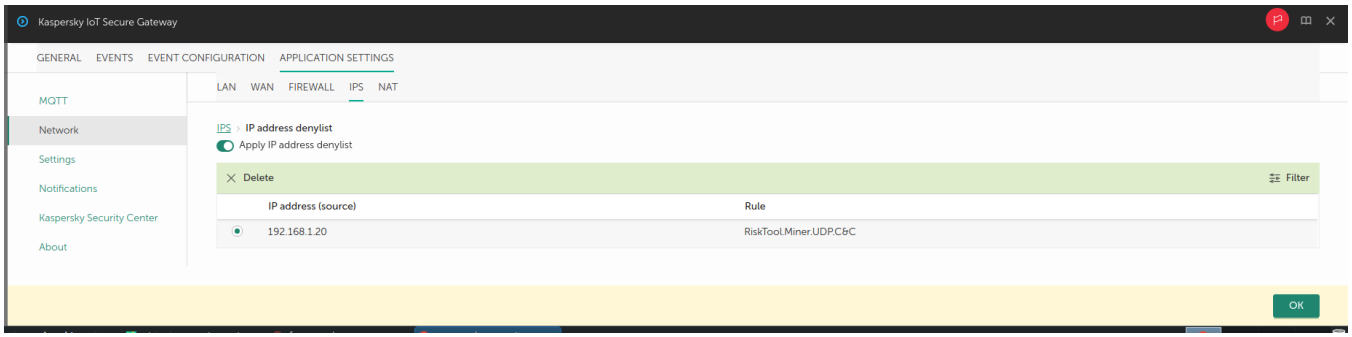
В перечне "BlockedListRules" появится хост с IP-адресом источника атаки.



Сетевые соединения между хостом "http_server_wan" и хостом с IP-адресом 10.65.144.80 будут заблокированы с помощью МСЭ на KISG.

Разблокировать устройство, попавшее в "BlockedListRules", можно следующими способами:

- подождать 60 минут. По истечении 60 минут ip-адрес заблокированного устройства удалится из "BlockedListRules";
- вручную удалить IP-адрес хоста "http_server_wan" из "BlockedListRules". 3. Удаление IP-адреса из списка разрешенных IP-адресов



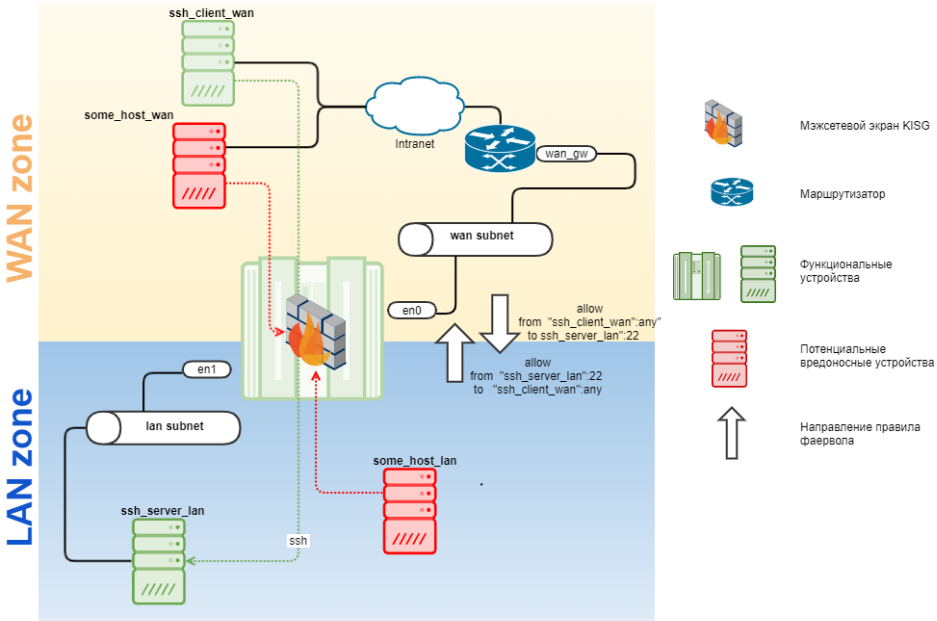
5.3. Описание схемы внедрения при работе KISG в режиме routing (режим маршрутизации пакетов)

Подробности настройки доступа из WAN-зоны в LAN-зону описаны в разделе 2. Сценарий: Настройка доступа из внешней сети к устройствам внутренней сети.

Далее будет приведен пример разграничения доступа для хоста "ssh_client_wan" к хосту "ssh_server_lan" по протоколу SSH. Последовательность действий по разграничению доступа можно условно разделить на 2 этапа:

1) настройка маршрутизации и проверка сетевой доступности;

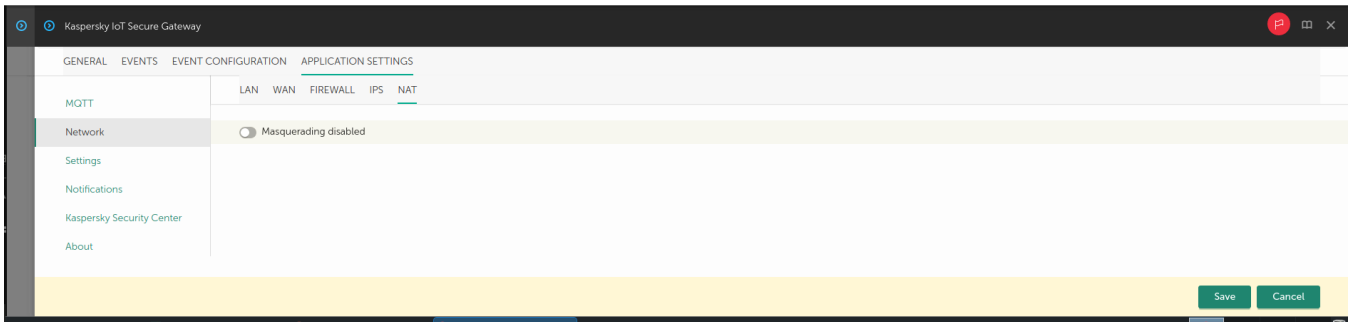
2) добавление правил МСЭ для LAN- и WAN-зон.



Рассмотрим каждый из этих этапов более детально.

5.3.1. Маршрутизация

Чтобы KISG начал маршрутизировать пакеты из WAN в LAN нужно с помощью plugin KSC выключить режим NAT. Для этого web-интерфейсе KSC нужно перейти в свойства управляемого KISG. Во вкладке "Application settings" → "Network" → "NAT" и переключить тумблер:



Подробности переключения: 7. Настройка маскарадинга

Затем необходимо убедиться в корректности настройки маршрутизации на сетевых устройствах, которые работают совместно с KISG. В частности это необходимо сделать на роутре, который стоит в WAN-зоне и маршрутизирует трафик в "intranet".

На маршрутизаторе должны быть следующие маршруты:

- из intranet в подсеть "lan subnet", указав в качестве шлюза ip-адрес WAN-интерфейса KISG (en0)
- маршрут от подсети "lan subnet" в сегмент intranet, указав в качестве шлюза интерфейс маршрутизатора "wan_gw".

Чтобы исключить пропажу маршрута на роутере рекомендуется настроить статический IP-адрес на WAN-интерфейсе KISG (en0). Настроить статический IP-адрес можно, руководствуясь 2. Настройка параметров внешней сети. Если WAN-интерфейс KISG будет получать IP-адрес по DHCP, то маршрутизация в LAN-подсеть собьется при смене IP-адреса WAN-интерфейса и потребуется обновлять правила маршрутизации на роутере.

Актуальные IP-адреса и маршруты для KISG можно узнать в web-интефейсе KISG на страничке https://192.168.1.1/troubleshooting.

Если маршрутизация настроена корректно, то хост "ssh_client_wan" должен иметь возможность выполнить ping до хоста "ssh_server_lan". Межсетевой экран KISG не блокирует ICMP-пакеты.

Перед подключением KISG к маршрутизатору желательно убедиться, что подсеть "wan subnet" на маршрутизаторе отличается от подсети "lan subnet". Многие маршрутизаторы часто работают с подсетью 192.168.1.0/24 как и LAN-интерфейс KISG.

5.3.2. Разграничение доступа для хоста из WAN-зоны при работе KISG в режиме работы "routing"

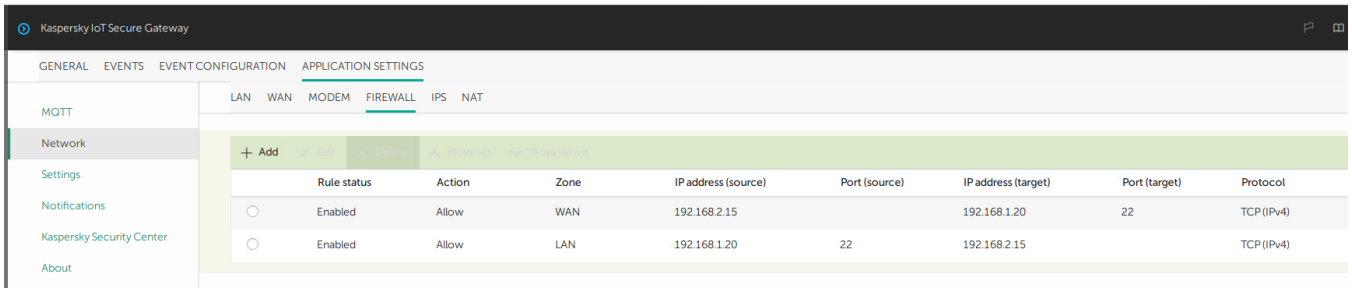
В отличии от режима работы KISG в режиме NAT необходимо добавить правило не только в LAN-зоне , но и в WAN-зоне.

Допустим у хоста "ssh_client_wan" IP-адрес 192.168.2.15, а у хоста "ssh_server_lan" IP-адрес 192.168.1.20. Предполагается, что устройства в LAN-зоне получают IP-адреса по DHCP. В таком случае стоит указать не конкретный адрес 192.168.1.20, а подсеть 192.168.1.0/24. Тогда в KISG необходимо настроить как минимум следующие правила МСЭ:

Действие	Зона / Протокол L4 / IP-адрес: Номер порта источника → IP-адрес :Номер порта назначения
Разрешить	- LAN / TCP / 192.168.1.0/24:22 → 192.168.2.15:any
Разрешить	- WAN / TCP / 192.168.2.15:any → 192.168.1.0/24:22

В данном случае требуется добавить два правила. Правило " WAN / TCP / 192.168.2.15:any → 192.168.1.0/24:22" является входящим stateful-правилом на wan-интерфейсе KISG. Правило "LAN / TCP / 192.168.1.0/24:22 → 192.168.2.15:any" играет роль входящего в LAN-зону stateless-правила. Необходимость добавления stateless-правила при разграничении доступа из WAN-зоны в LAN-зону вызвано архитектурными особенностями реазиции МСЭ в KISG.

Итоговый перечень правил МСЭ в консоли KSC будет выглядеть следующим образом:

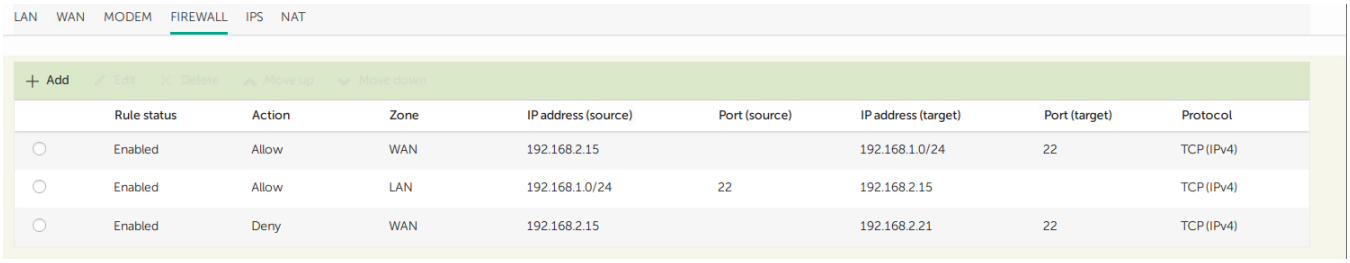


После добавления правил из WAN-зоны в LAN-зону их применения может потребоваться перезагрузка KISG.

5.3.3. Добавление запрещающего deny-правила для хоста из WAN-зоны при работе KISG в режиме работы "routing"

Если для хоста в WAN-зоне требуется ограничить доступ в LAN-зону, то нужно добавать deny-правило совместно с разрешающими правилами:

Действие	Зона / Протокол L4 / IP-адрес: Номер порта источника → IP-адрес :Номер порта назначения
Разрешить	- LAN / TCP / 192.168.1.0/24:22 → 192.168.2.15:any
Разрешить	- WAN / TCP / 192.168.2.15:any → 192.168.1.0/24:22
Запретить	- WAN / TCP / 192.168.2.15:any → 192.168.1.21:22

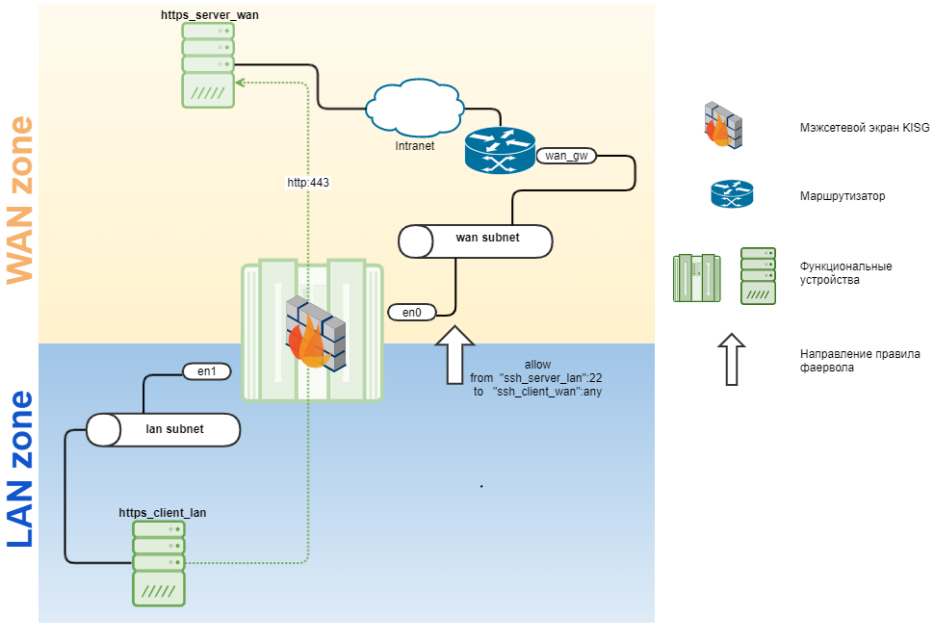


После синхронизации настроек между KSC и KISG хост "ssh_client_wan" потеряет возможность подключиться к "ssh_server_lan".

После применения такого правила может потребоваться перезагрузка KISG.

5.3.4. Разграничение доступа для хоста из LAN-зоны при работе KISG в режиме работы "routing"

Разграничение из LAN-зоны в WAN-зону в режиме "routing" не отличается подхода по разграничению доступа в режиме NAT.



Допустим у хоста "https_client_lan" IP- адрес 192.168.1.20, а хоста "https_server_wan" IP-адрес 10.65.144.80. Если нужно разграничить доступ для хоста "https_client_wan" на "https_server_wan" по порту 443, то правило МСЭ будет выглядеть примерно следующим образом:

Действие	Зона / Протокол L4 / IP-адрес: Номер порта источника → IP-адрес :Номер порта назначения
Разрешить	- LAN / TCP / 192.168.1.20:any → 10.65.144.80:443

5.4. Настройка KISG в режиме "modem"

ВАЖНО!

- Sim-карта, установленная в UTX-3117, должна поддерживать работу через модем. Уточнить тарифный sim-карты и перевести ее режим работы "модем" можно, обратившись к оператору связи;
- хост в LAN-зоне должен получить настройки сети от DHCP-сервера KISG, чтобы устройство в LAN-зоне получить доступ в интернет через модем KISG .

Для работы с модемом необходимо настроить профиль беспроводного соединения. По умолчанию в KISG предустановлены профили для работы с операторами "MTS", "Beeline", "Megafon". Можно выбрать уже существующий профиль из перечня предуставновленны (для операторов MTS, Beeline, Megafon) или сделать новый профиль (3. Создание нового профиля модема). Создавать новый профиль нужно, если настройки оператора отличаются от стандартых.

После создания профиля необходимо сделать нужный профиль активным (1. Таблица профилей модема) , перезапустить KISG и включить беспроводной режим передачи данных 2. Включение и выключение беспроводного соединения.

Примеры конфигурационный файлов PPP для операторов "MTS", "Beeline", "Megafon" можно изучить в web-интерфейсе KISG. Эти конфигурационные файлы готовы для настройки беспроводного соединения с мобильным оператором через модем.

Подробнее про работу протокола PPP можно почитать:
http://www.bsdportal.ru/fdocs/books/handbook/userppp.html

Примеры конфигурационных файлов PPP:
https://github.com/FreeBSDDesktop/freebsd-base/tree/master/share/examples/ppp

6. Определение схемы подходящей схемы внедрения

При подборе схемы внедрения KISG стоит учитывать следующие факторы в зависимости от режима работы:

NAT	**Routing**
Необходимо учитывать, что правила можно создавать только по IP-адресам	Необходимо учитывать, что правила можно создавать только по IP-адресам
Производится помена ip-адреса при прохождении пакета из зоны LAN в зону WAN через KISG	Для доступа в LAN на маршрутизаторе в WAN-зоне необходимо прописать маршрут в LAN подсеть через WAN-интерфейс KISG. В таком случае на KISG лучше настроить статическую маршрутизацию.
Нет возможности получить доступ из WAN-зоны в LAN-зону	Правила МСЭ нужно прописать как для LAN-зоны , так и для WAN-зоны
Правила МСЭ достаточно прописать для LAN-зоны	

Ниже приведена схема, отображающая возможные информационные потоки. Данная схема поможет сориентироваться с тем для каких хостов потребуется создавать правила МСЭ, а какие хосты будут работать без ручных правил МСЭ. Зеленым и синим цветом выделены устройства, для которых действуют разрешающие служебные правила. Для серых и красных устройств действует запрещающее правила "default deny any: any->any:any" .

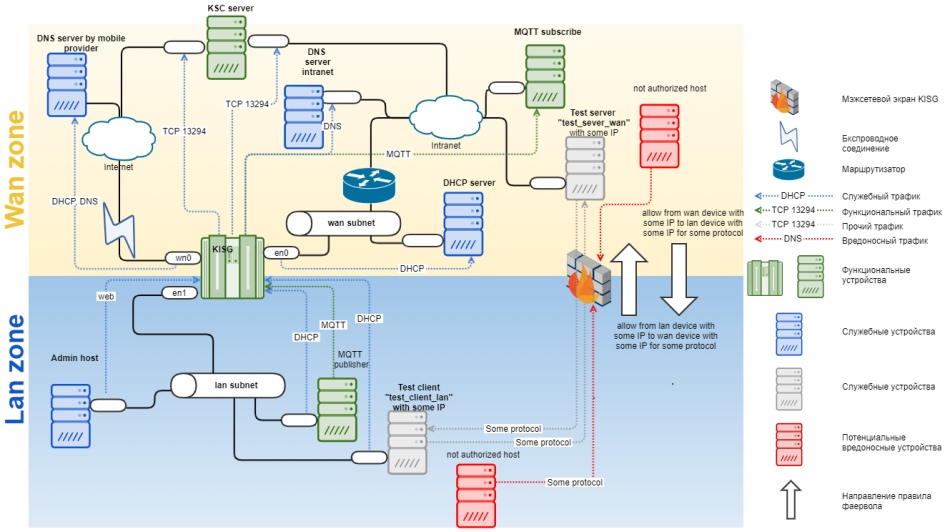


Рисунок 2 - Типовая схема установки KISG с включенной маршрутизацией