robustel

Ниеншанц
Автоматика

MG460

Шлюз кибербезопасности для судового оборудования

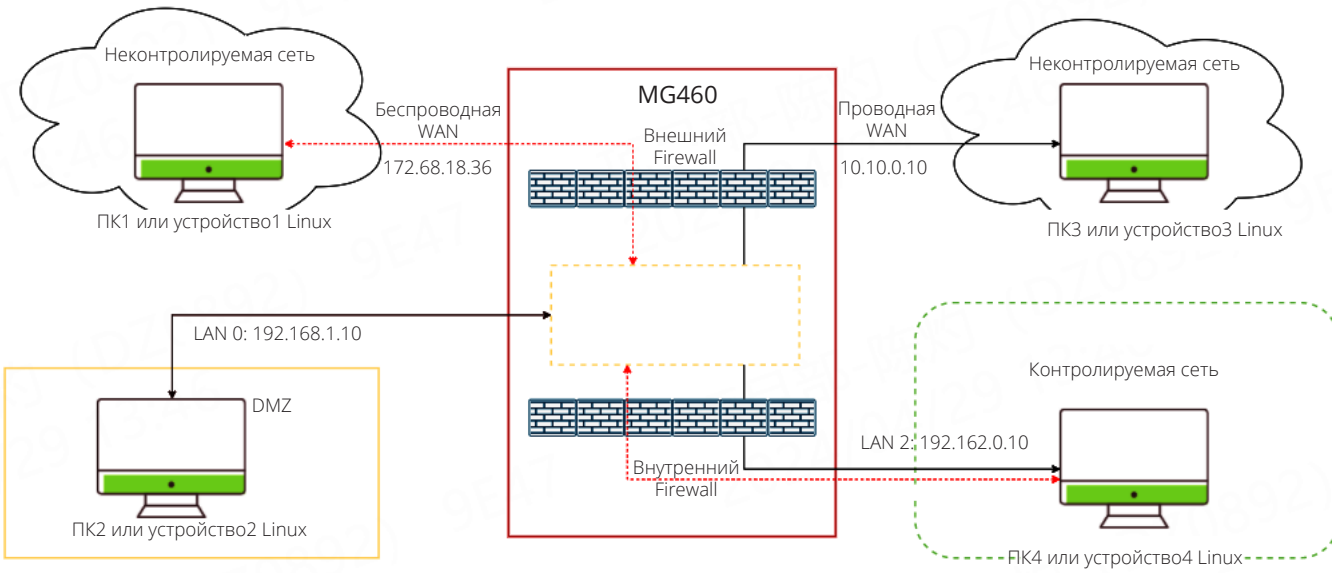
Руководство по безопасности

ОГЛАВЛЕНИЕ

Глава 1. ОБЗОР ИЗДЕЛИЯ

Robustel MG460 — это новое поколение промышленных шлюзов для морского транспорта, соответствующих стандартам IEC61162–460 (Морское навигационное оборудование. Безопасность и защита) и IEC60945. MG460 можно использовать как шлюз между бортовым оборудованием судна и внешними сервисами (облачные платформы, серверы и т. п.).

MG460 предназначен для обеспечения безопасности сети морского транспорта. MG460 предоставляет многоуровневый межсетевой интерфейс и контроль доступа на сетевом/транспортном уровне на основе адресов, портов и протоколов. Шлюз, как один из важнейших компонентов сети, нацелен на обеспечение соответствия современным требованиям морской отрасли.



Весь трафик из неконтролируемых сетей передается или обрабатывается через MG460, который состоит из межсетевых интерфейсов и DMZ с различными серверами. DMZ расположен между внутренней сетью 460 и неконтролируемой сетью. 4 зоны firewall: внешний — для неконтролируемой, внешней, сети; внутренний — для сети 460, и два firewall (input/output) самого устройства.

Глава 2. ОПИСАНИЕ БЕЗОПАСНОСТИ

1. **MG460 не предназначен для организации доступа в Интернет для экипажа.**
2. **Авторизация: без авторизации нельзя изменить настройки.**
   - Требования к паролю:

Для изменения настроек устройства предусмотрен механизм аутентификации пользователя.

В пароле используются как минимум три из четырех доступных типов символов: строчные буквы, заглавные буквы, цифры и специальные символы.

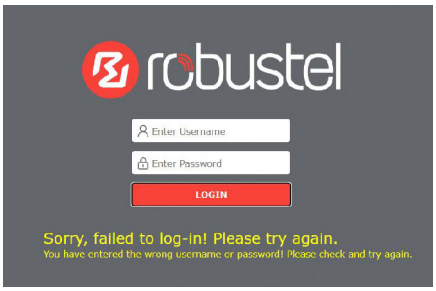
Пароль содержит не менее 8 символов.

Пароль не содержит имени пользователя или частей полного имени пользователя, таких как имя, название компании, название изделия и т. п.; словарные слова не используются. Следует использовать пароли, состоящие из случайного набора символов и не имеющие смыслового значения.

- Использование HTTPS и хранение паролей в зашифрованном виде:

Для доступа к веб-интерфейсу используется шифрование SSL. В файлах настроек пароли хранятся в зашифрованном виде.

- При вводе неверного имени пользователя или пароля появляется следующее предупреждение:



- Наличие уровня привилегий для пользователя:

По умолчанию шлюз имеет только одного пользователя с правами администратора и уникальным паролем.

- Автоматический выход:

При отсутствии активности в веб-интерфейсе в течение 15 минут производится автоматический выход из системы.

- Регистрация попыток авторизации:

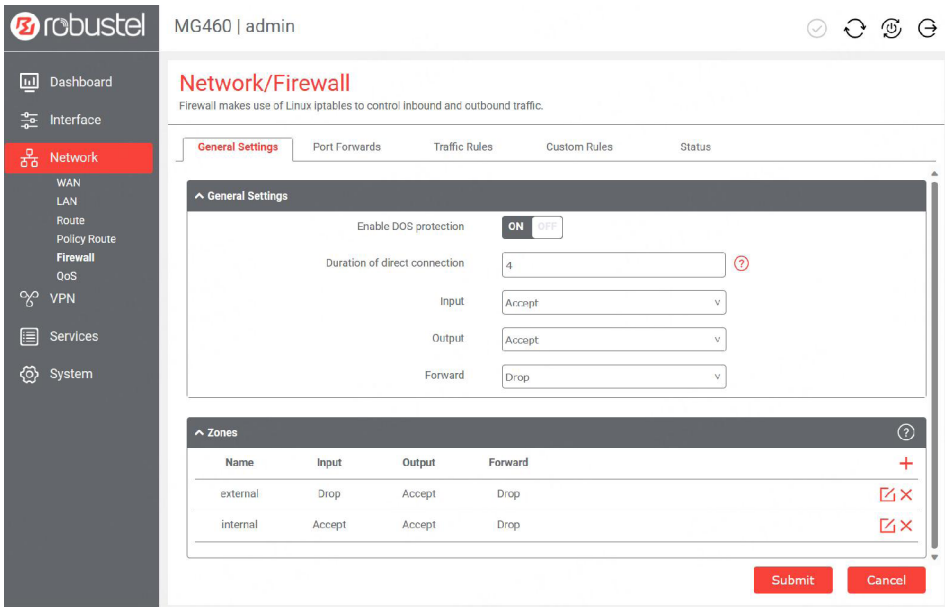
Все попытки авторизации регистрируются в специальном журнале.

Для проверки настроек устройства создается учетная запись с правами только на чтение:

Login: admin

Password: Guest123

3. Firewall:



- Политика по умолчанию — DROP:

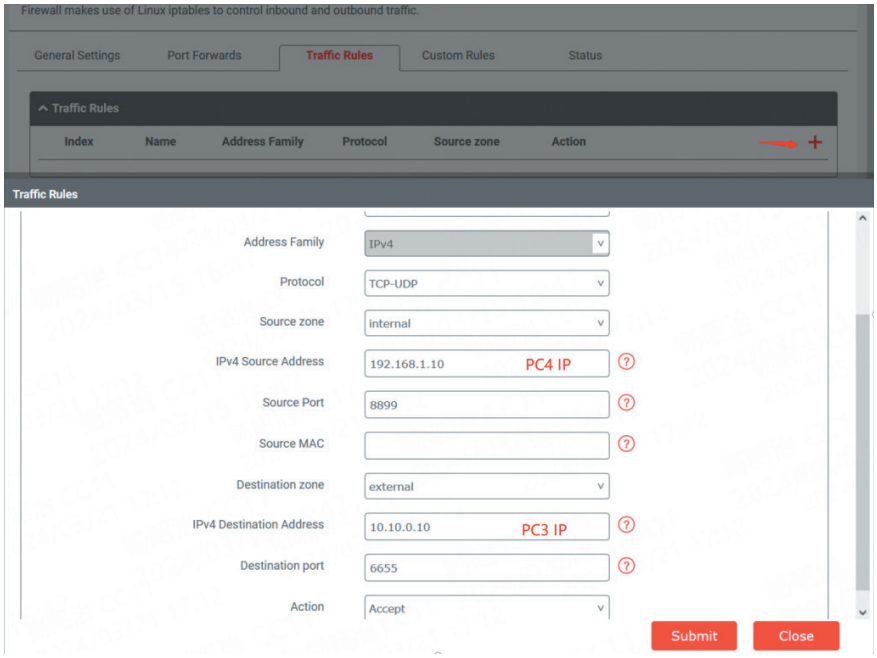
По умолчанию firewall блокирует ВСЕ внешние подключения, кроме явно разрешенных.

- Для защиты от DoS-атак пакеты ICMP/IGMP передаются не чаще 3 пакетов в секунду, остальные блокируются.
- Цели и задачи DMZ:

DMZ предназначена для обеспечения безопасной внутренней мостовой сети. DMZ представляет собой сервер приложений с ограниченным доступом к Интернету (только серверы компании) и без доступа к внутренней мостовой сети. Станция из внутренней сети инициирует подключение к серверу приложений для приема данных.

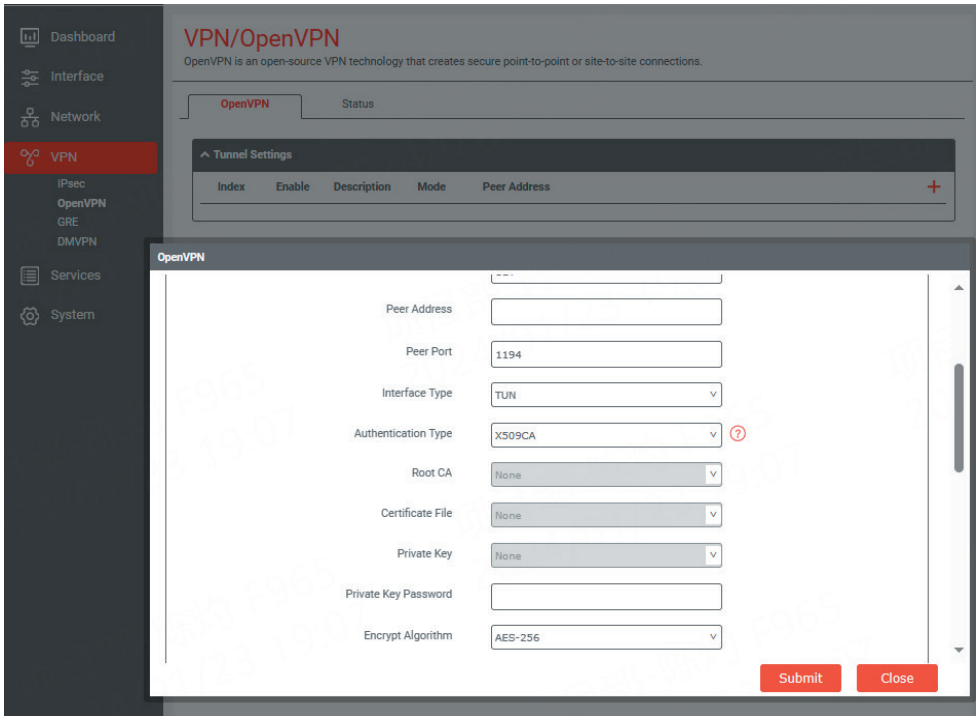
Для организации firewall DMZ имеет два набора правил для фильтрации трафика между сетью 460 <-> DMZ и DMZ <-> Интернет.

- Правила firewall содержат исходный IP-адрес, IP-адрес назначения, порты источника/назначения и протокол:



4. Прямое подключение (удаленная поддержка в нашем понимании):

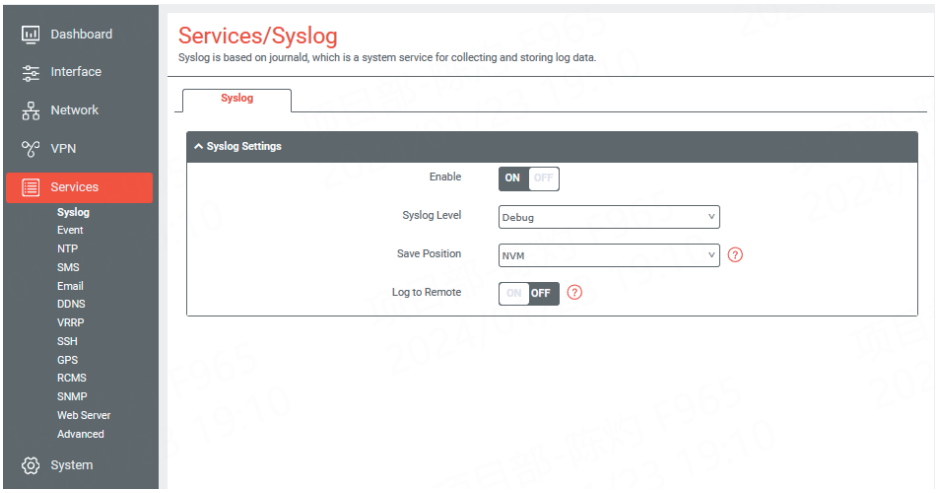
- По умолчанию подключение VPN выключено. Сервисный инженер делает запрос на удаленное подключение к мосту и подключается к сети VPN через внутренний портал. Решение о возможности подключения принимает капитан, с помощью специально подключенной кнопки он может разрешать или прерывать VPN соединение.
- Для поддержки используется VPN с шифрованием AES и ключом в 256 бит:



- Алгоритм удаленного подключения: запрос через удаленный сервис, без одобрения со стороны судна подключение не осуществляется.
- Тайм-ауты: Реализовано ограничение длительности сессии: 10 минут для сессии без переданных пакетов и 4 часа (настраиваемый параметр) для прямого подключения. Прямое соединение также можно принудительно разорвать по правилам стандарта ECDIS.

5. Системный журнал:

MG460 ведет журнал всех важных событий в системе. Для дублирования записей журнал передается на мостовую станцию и сервер приложений.



- Шлюз хранит журналы в NVM (энергонезависимой памяти).
- Как правило, размер журнала для одного события составляет менее 100 байт. При 20 000 событий общий объем хранилища журналов составит примерно 2 МБ. В MG460 установлена карта памяти eMMC на 64 Гб, что обеспечивает достаточную емкость для хранения данных. Учитывая что системные журналы будут храниться в течение 12 месяцев, емкость более чем достаточна для размещения всех системных журналов в течение этого периода времени.

6. Обновление прошивки:

- Только авторизованные пользователи могут обновить прошивку.
- Офлайн-метод с использованием флэш-памяти: требуется файл ключ на основе пароля.
- Онлайн-метод через веб-интерфейс: System->App center.
- Перед обновлением прошивки система автоматически проверяет цифровую подпись файла, что защитит систему от установки несанкционированного или поврежденного ПО.
- Для удаленного обслуживания ПО необходимо заранее установить VPN-соединение. Пользователь на судне должен настроить VPN, чтобы авторизованные удаленные пользователи могли получать доступ к устройству и выполнять обновления прошивок.
- Когда происходит обновление прошивки, всплывающее окно уведомляет пользователя об успешном или неудачном завершении обновления. Если обновление завершится неудачно, это не повлияет на работу шлюза. MG460 сохранит свои прежние настройки и продолжит работать в прежнем режиме.
- Robustel придерживается практики управления жизненным циклом ПО согласно стандартам CMMI (Capability Maturity Model Integration) и требованиям IEC62443–1.
- Управление версиями прошивок:

V 2.1.3

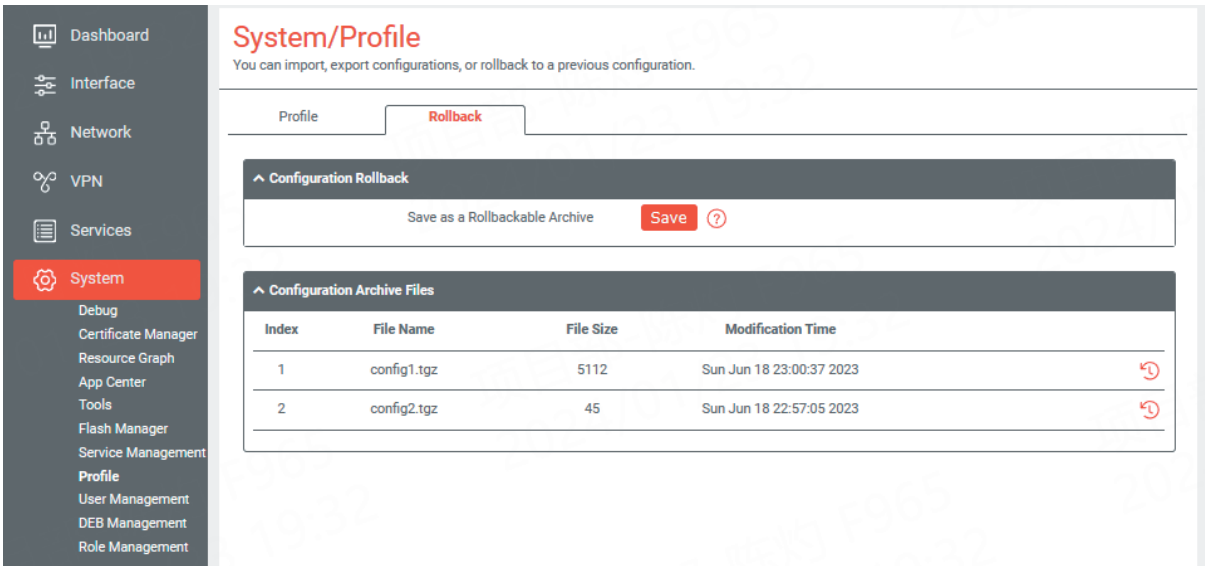
- Основная итерация: При значительных изменениях в архитектуре прошивки, таких как переход с Debian на Ubuntu, версия обновляется с версии V2.x.x до V3.x.x.
- Новый функционал: При появлении новой функции версия обновляется с V2.1.x до V2.2.x.
- Регулярное устранение уязвимостей: Стандартные исправления ошибок в прошивках устраняются незамедлительно, в таких случаях версия обновляется с V2.1.3 до V2.1.4, чтобы показать на исправление ошибки без внесения существенных изменений.

- Выпуск новых версий прошивки: прежде всего ПО проходит тщательные тесты внутренней командой тестировщиков. При необходимости перед выходом ПО на рынок проводятся тесты на стороне заказчика.

7. Обновление профиля:

- Офлайн-метод с использованием флэш-памяти: требуется файл ключа на основе пароля.
- Онлайн-метод через веб-интерфейс.
- Система автоматически создаст точку сохранения, если изменения конфигурации будут сохранены и применены.

Для отката перейдите на страницу System -> Profile -> Rollback



8. Беспроводные возможности шлюза MG460.

- В шлюзе MG460 LTE-модем настроен как WAN-интерфейс с теми же настройками доступа и ограничениями, что в основном WAN-интерфейсе — входящие соединения запрещены, вся связь с внешним миром осуществляется только через зашифрованные https/VPN.
- Точка доступа Wi-Fi не поддерживается.

9. Интерфейс BAM

- Приложение BAM interface — это приложение, обеспечивающее сетевой интерфейс связи между шлюзом MG460 и системой Bridge Alert Management (BAM) в соответствии с требованиями стандарта IEC 62923–1 ed.1.
- MG460 используется в качестве оборудования, совместимого с BAM типа «P», и передает предупреждения только в систему BAM.
- MG460 поддерживает только отправку сообщений HBT и ALF в систему BAM и не принимает сообщения подтверждения.
- Когда будет установлено прямое соединение (включен VPN), EUT отправит сообщение ALF в систему BAM.

10. Шлюз MG460 оснащен тремя USB-портами, но по умолчанию все USB-порты отключены. Однако порты USB-хоста могут быть включены для обновления прошивки или настроек. Для выполнения этих обновлений для аутентификации требуется файл защищенного ключа. После завершения обновления у пользователей будет возможность снова отключить все USB-порты, а порт USB OTG оставить для доступа пользователя к microSD при необходимости.

11. MG460 — это отдельный компонент, а не система 460, он не выполняет синхронизацию времени сам по себе. Он выполняет синхронизацию для себя через NTP / GNSS, может быть NTP сервером.

Основные характеристики

- Соответствие стандартам IEC61162–1, IEC61162–2, IEC 61162–460 и IEC 60945
- Высокостабильная сотовая связь 4G/3G/2G с охватом всего диапазона
- Высокопроизводительный вычислительный модуль с процессором 1,6 ГГц + флэш-память eMMC объемом 64 ГБ для запуска сложных приложений.
- Wireguard/IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN + дополнительные опции VPN
- Поддержка контейнеризации Docker
- 5 портов Ethernet 1000 Мбит/с
- 2 порта RS-232/RS-422/RS-485 (с программной настройкой) для подключения к промышленным/устаревшим устройствам.
- 2 дискретных входа и 2 релейных выхода для простого мониторинга и управления.
- 2 × USB3.0 тип A, 1 × USB2.0 тип C
- Два слота для SIM-карт для резервного обмена данными.
- Широкий диапазон рабочих температур для промышленного применения
- Поддержка C, C++, Python, Java, Node.js и др. (для разработки приложений пользователя)
- В настоящее время доступно более 50 000 приложений из репозитория Debian
- Поддержка RCMS (платформы управления маршрутизаторами/шлюзами Robustel) для эффективного управления большим количеством устройств через службу RobustVP N.

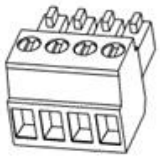
Комплект поставки

Перед установкой шлюза MG460 проверьте комплектность.

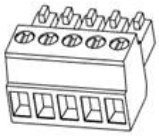
Примечание: Следующие изображения приведены исключительно в иллюстративных целях и не отражают фактических размеров.

- Шлюз кибербезопасности для судового оборудования Robustel MG460–1 шт.

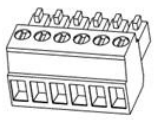
- 4-контактная клеммная колодка 3,5 мм — 1 шт.



- 5-контактная клеммная колодка 3,5 мм — 1 шт.

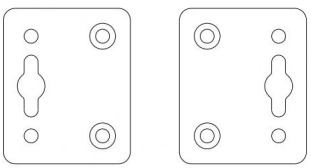


- 5-контактная клеммная колодка 3,5 мм — 1 шт.



- 1 комплект для настенного монтажа или 1 комплект для монтажа на DIN-рейку (в соответствии с фактическими требованиями заказа)

Комплект для монтажа на DIN-рейку монтажа



Комплект для настенного

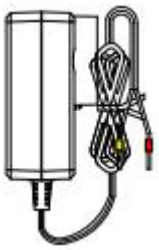
Примечание: Если какой-либо из указанных компонентов отсутствует или поврежден, обратитесь к торговому представителю Robustel.

Дополнительное оборудование (продается отдельно):

- Антенна сотовой связи 4G SMA

- Антенна WiFi RP-SMA (короткая/на магн. основании, дополнительно)

- Адаптер питания AC/DC (24 В пост. тока, 1 А; вилка EU/US/UK/AU дополнительно)



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Основные характеристики шлюза

- Процессор: Quad core Cortex-A53, 1,6 ГГц
- Флэш: 64 ГБ eMMC · ОЗУ 4 ГБ DDR4

Сотовый интерфейс

- Количество антенн 4G: 2
- Разъем SMA-K
- SIM: 2 × Mini SIM (2FF)

Интерфейс GNSS

- Количество антенн: 1
- Технология GNSS: GPS/GLONASS/BeiDou/Galileo/QZSS (дополнительно)

Интерфейс Ethernet

- Порты: 5 × RJ45, 10/100/1000 Мбит/с, соответствие стандартам 1000BAST-T, магнитная изоляция LAN или WAN · Защита: 1 кВ

Последовательный интерфейс

- Тип: 2 порта RS232/RS422/RS485 (с программной настройкой)
- Разъем 2 6-контактных 3,5 мм, защита от электростатического разряда 8 кВ возд., 4 кВ конт., скорость передачи данных от 300 до 115200 бит/с RS232: TXD, RXD, GND RS485: Data+ (A), Data- (B), GND RS422: A, B, Y, Z, GND

Интерфейс консоли

- Тип: 1 × RS232 разъем RJ45 скорость передачи данных от 300 до 115200 бит/с
- Сигнал: TXD, RXD, GND

Интерфейс дискретного входа (DI)

- Порты: 2 × DI разъем 4-контактный 3,5 мм, «мокрый контакт»
- Изоляция: Двунаправленная оптопара (DI). Макс. напряжение +30 В пост. Макс. ток 100 мА
- Определение сигнала: DI1+, DI1-, DI2+, DI2-

Интерфейс релейного выхода

- Порты: 2 релейных выхода разъем 4-контактный 3,5 мм, макс. напряжение +48 В пост. Макс. ток 100 мА
- Определение сигнала: NC1, NO1, COM1, NC2, NO2, COM2

Интерфейс USB

- Порты: 2 × USB 3.0 (хост), Тип A, 5 В 900 мА, 1 × USB 2.0 (OTG), тип C

Другое

- SD: 1 × microSD
- HDMI: 1 × HDMI
- Кнопка RESET: 1 × RST
- Светодиодные индикаторы: 1 × RUN, 1 × MDM, 2 × USR, 1 × Signal, 1 × VPN
- Сторожевой таймер: Внешний

Физические параметры

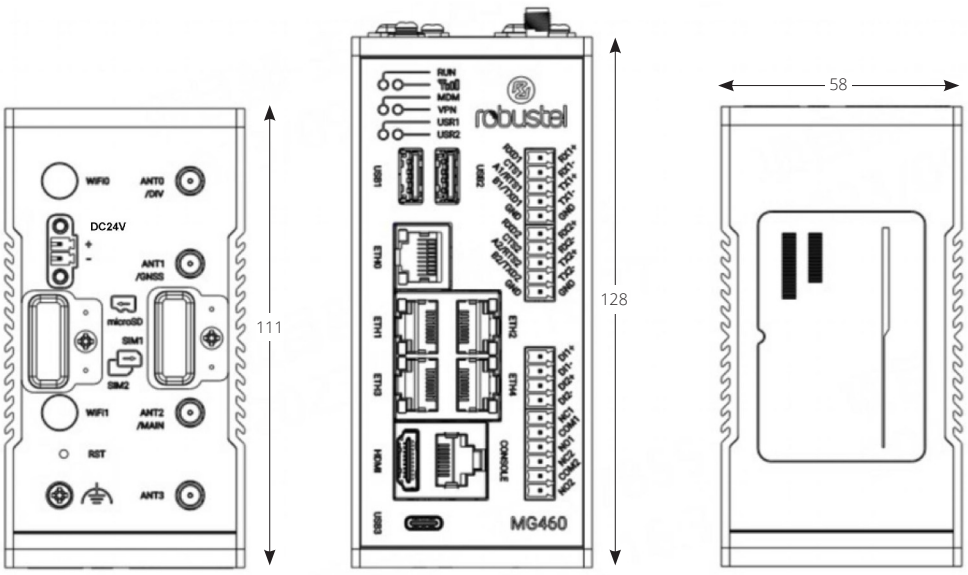
- Класс защиты IP30
- Корпус: Металл
- Размеры: 60 × 105 × 128 мм
- Монтаж: На стол, на стену, на DIN-рейку 35 мм
- Рабочая температура: от –40 до +70 °C
- Температура хранения: от –40 до +85 °C
- Относительная влажность: 5–95%

Источник питания и потребляемая мощность

- Разъем 2-контактный 3,5 мм с фиксацией
- Входное напряжение: 24 В пост. тока (+30%/–10%)

Размеры

- 58 × 111 × 128 мм (ширина × глубина × высота)



Вид сверху Вид спереди Вид снизу

Глава 3. УСТАНОВКА ОБОРУДОВАНИЯ

Разводка контактов

Последовательные порты Два программно-конфигурируемых последовательных порта, которые можно настроить как RS-232, RS-422 или RS-485.

Название	Режим RS232	Режим RS485
TXD1/A1	отправка данных	RS485_A
RXD1/B1	получение данных	RS485_B
GND1	Заземление	Заземление
TXD2/A2	отправка данных	RS485_A
RXD2/B2	получение данных	RS485_B
GND2	Заземление	Заземление

Порты Ethernet

Порты Ethernet. 5 портов Ethernet, которые можно настроить как WAN или LAN.

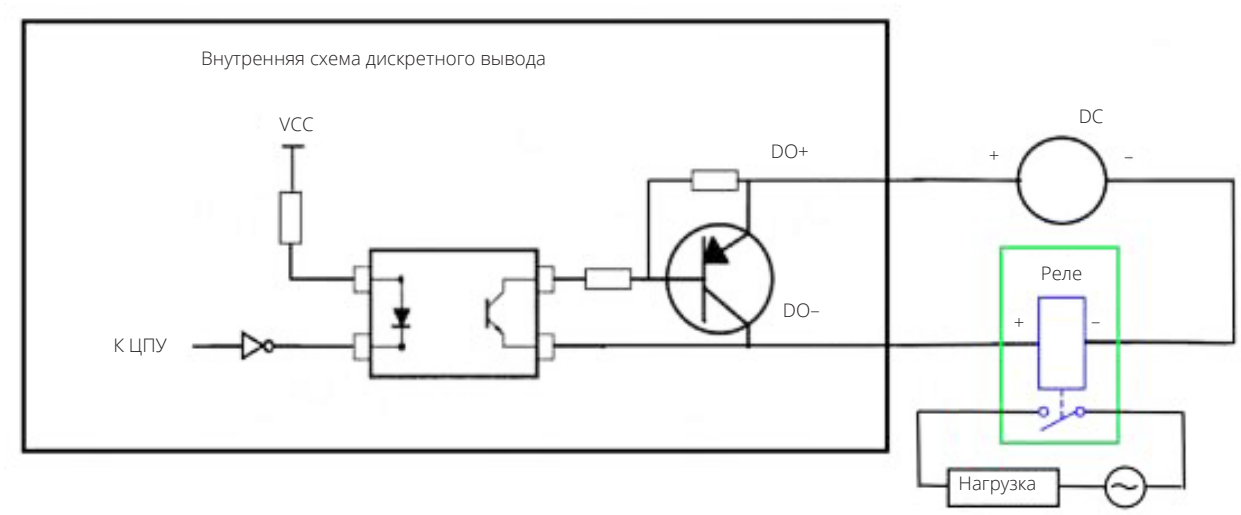
	Светодиод	Описание
Activity	Вкл., мигает	Передача данных
	Выкл.	Нет действий
Link	Выкл.	Канал выключен
	Вкл.	Канал включен

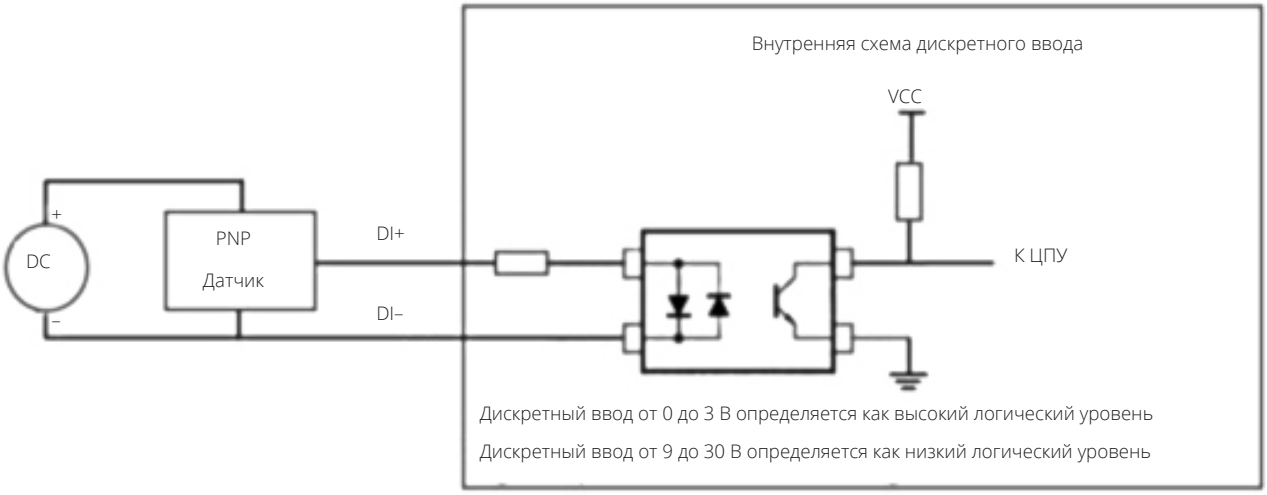
Кнопка Reset

Нажать и отпустить	СВЕТОДИОД RUN	Действие
Удерживать не больше 3 секунд	Вкл., затем регулярно мигает	Сброс
Удерживать больше 3, но меньше 10 секунд	Мигает регулярно -> мигает быстро	Сброс к заводским настройкам и перезагрузка
Удерживать больше 10 секунд	Горит 5 секунд, затем мигает регулярно	Нет действий

Порты дискретного ввода и вывода

Два набора дискретных входов и два набора дискретных выходов. Примеры применения приведены ниже.



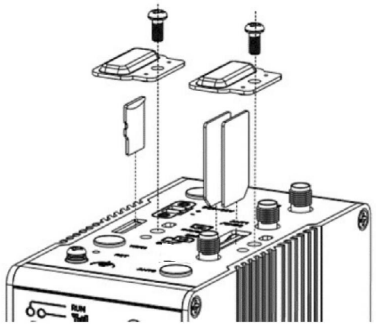


Примечание: Диапазон внешнего источника питания — от 5 до 30 В пост. тока, макс. 0,1 А.

Светодиодные индикаторы

Светодиод	Описание	
RUN	Вкл., горит постоянно	Инициализация шлюза
	Вкл., мигает	Шлюз начинает работу
	Выкл.	Питание шлюза выключено
MDM	Цвет	С модулем 4G: 2G: красный, 3G: желтый, 4G: Зеленый С модулем 5G: 3G: красный, 4G: желтый, 5G: Зеленый
	Вкл., мигает	Канал работает
	Выкл.	Канал не работает
	Зеленый	Сильный сигнал
	Желтый	Средний сигнал
	Красный	Слабый сигнал или нет сигнала
VPN	Вкл., горит постоянно	VPN соединение установлено.
	Выкл.	VPN соединение не установлено.
USR1/USR2	Определяется пользователем. Для получения более подробной информации, пожалуйста, обратитесь к руководству RT_SM_RobustOS Pro_Software Manual: **Services > Advanced > System >System Settings > User LED Type.**	

Установка SIM-карты



Установка SIM-карты

1. Убедитесь, что питание шлюза выключено.
2. Чтобы снять крышку слота, с помощью отвертки отверните винты, крепящие крышку, а затем найдите слот для SIM-карты.
3. Чтобы вставить SIM-карту, нажмите на нее пальцем до щелчка.
4. Установите крышку на место и затяните винты, крепящие ее, с помощью отвертки.

Извлечение SIM-карты

1. Убедитесь, что питание шлюза выключено.
2. Чтобы снять крышку слота, с помощью отвертки отверните винты, крепящие крышку, а затем найдите слот для SIM-карты.
3. Чтобы извлечь SIM-карту, нажмите на нее пальцем, пока она не выскочит, а затем извлеките карту.
4. Установите крышку на место и затяните винты, крепящие ее, с помощью отвертки.

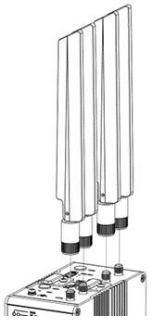
Примечание:

1. Рекомендуемый момент затяжки составляет 0,5 Н·м, а максимально допустимый — 0,7 Н·м.
2. Используйте специальную карту для работы устройства при экстремальных температурах (температура превышает 40 °C), поскольку обычная карта при длительной работе в суровых условиях будет часто отключаться.
3. Не забудьте плотно закрутить крышку, чтобы избежать кражи.
4. Не прикасайтесь к металлической поверхности карты, так как это может привести к потере или повреждению информации на карте.
5. Не сгибайте и не царапайте карту.
6. Держите карту вдали от источников электромагнитных полей.
7. Перед тем как вставлять или извлекать карту убедитесь, что питание шлюза выключено.

Подключение внешней антенны (тип SMA)

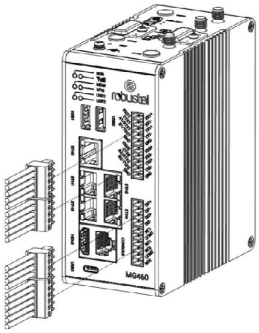
Подключите внешнюю антенну SMA к антенному разъему шлюза и плотно затяните. Убедитесь, что антенна имеет диапазон частот, соответствующий диапазону, предоставленному интернет-провайдером.

Примечание: Рекомендуемый момент затяжки — 0,35 Н·м.



Установка клеммной колодки

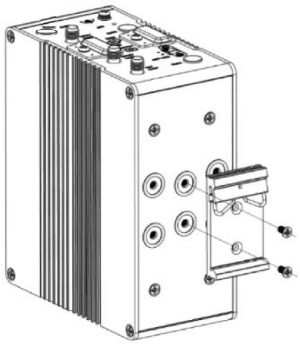
Вставьте 4-, 5- и 6-контактные клеммные колодки в разъем интерфейсов, после чего можно подключить устройства или датчики к шлюзу с помощью проводов через соответствующие интерфейсы, например, RS-232/RS-485, DIDO...



Монтаж

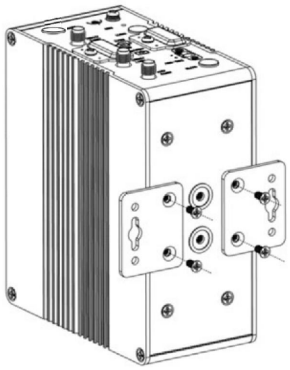
Монтаж на DIN-рейку

Используйте 2 винта M3 для крепления к устройству кронштейна для монтажа на DIN-рейку, затем повесьте устройство на DIN-рейку.



Монтаж на стену

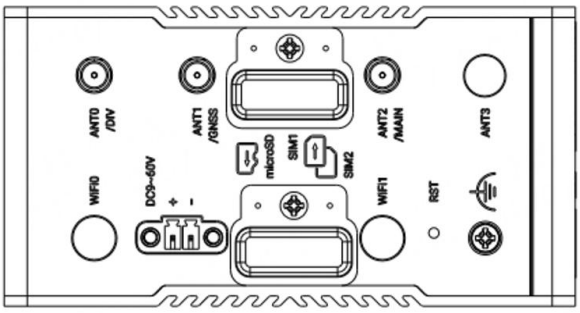
Используйте 2 винта M3 для крепления к устройству пластин для монтажа на стену, затем повесьте устройство на стену.



Заземление устройства

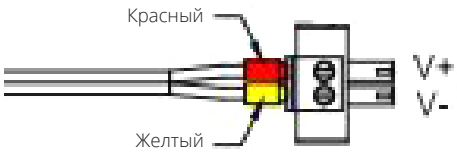
Заземление помогает предотвратить шумовые эффекты, вызванные электромагнитными помехами (EMI). Перед включением питания подключите устройство к заземляющему проводу на объекте с помощью винта заземления.

Примечание: Данное изделие подходит для установки на надежно заземленную поверхность, например, на металлическую панель.



Установка источника питания

При необходимости вставьте шнур питания в соответствующую клеммную колодку, затем вставьте клеммную колодку в разъем питания.

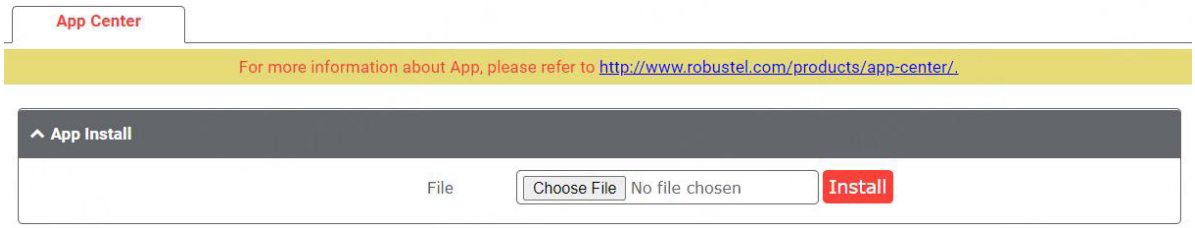


MG460 поддерживает защиту от обратной полярности. Подключайте адаптер питания правильно, в соответствии с рисунком выше. От адаптера питания идут два провода, в соответствии с цветом наконечника подключите кабель, обозначенный красным, к положительному полюсу через клеммную колодку, а желтый подключите к отрицательному полюсу таким же образом. Заключительный шаг — включить адаптер питания в розетку.

Примечание: Диапазон напряжения питания 24 В пост. тока (+30%/–10%).

Обновление системы

В этом разделе описано обновление прошивки шлюза. Щелкните System -> App Center, затем щелкните Choose File, чтобы выбрать файл прошивки, который будет использован для обновления. После выбора файла щелкните Update, чтобы запустить процесс обновления. Процесс обновления может занять несколько минут. НЕ ВЫКЛЮЧАЙТЕ шлюз в процессе обновления прошивки.

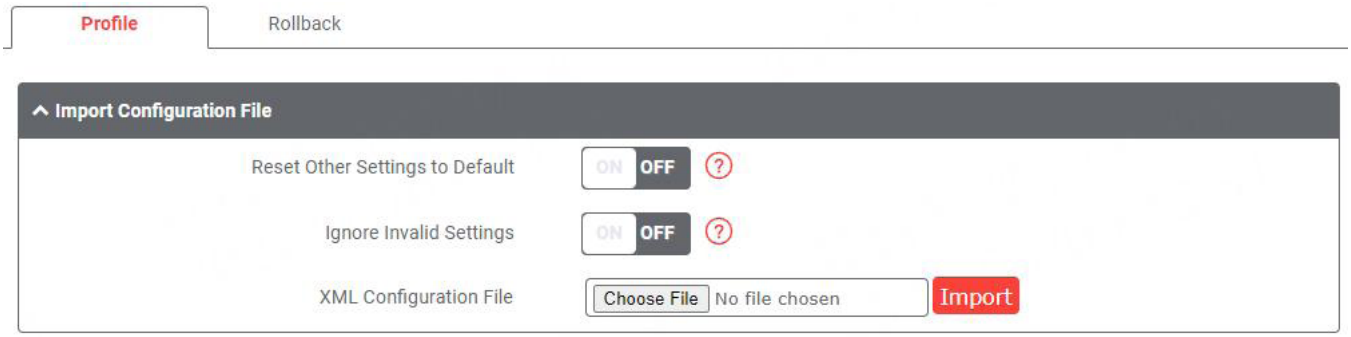


Примечание: Для получения файла последней прошивки обратитесь в техническую поддержку.

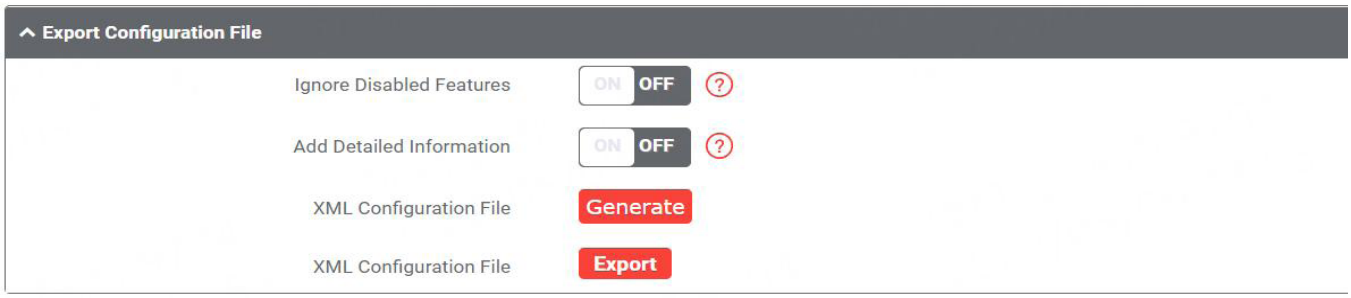
Глава 4. ОБНОВЛЕНИЕ ПРОФИЛЯ

Этот раздел описывает импорт и экспорт файла конфигурации и восстановление заводских настроек устройства. Щелкните System -> Profile

Профиль



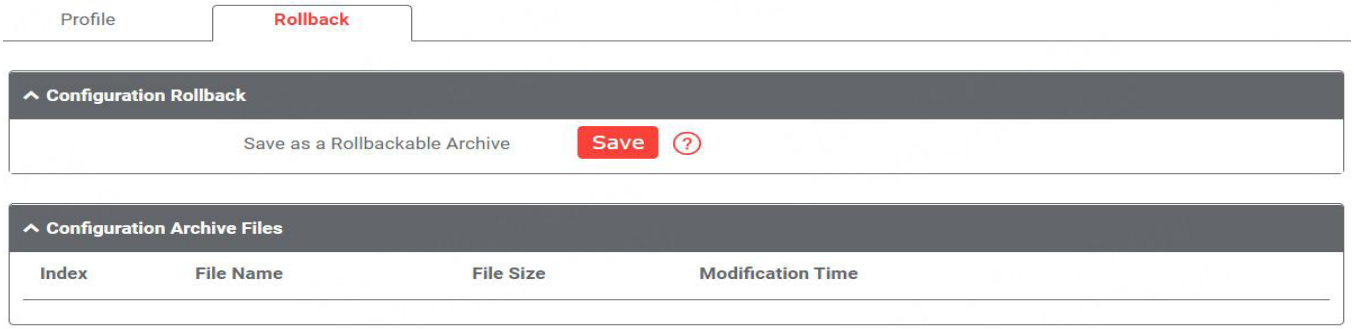
Элемент	Описание	По умолчанию
Reset Other Settings to Default	Щелкните переключатель в положение ON, чтобы вернуть другие параметры к настройкам по умолчанию.	OFF
Ignore Invalid Settings	Щелкните переключатель в положение ON, чтобы игнорировать недопустимые настройки.	OFF
XML Configuration File	Щелкните Choose File, чтобы выбрать XML-файл конфигурации на ПК, затем щелкните Import, чтобы импортировать файл в устройство.	—



Элемент	Описание	По умолчанию
Ignore Disabled Features	Щелкните переключатель в положение OFF, чтобы игнорировать отключенные функции.	OFF
Add Detailed Information	Щелкните переключатель в положение ON, чтобы добавить подробную информацию.	OFF
Encrypt Secret Data	Щелкните переключатель в положение ON, чтобы зашифровать секретные данные.	ON
XML Configuration File	Щелкните кнопку Generate для создания XML-файла конфигурации, затем щелкните Export для экспорта XML-файла конфигурации.	—

Элемент	Описание	По умолчанию
Save Running Configuration as Default	Щелкните кнопку Save, чтобы сохранить текущие параметры как конфигурацию по умолчанию.	—
Restore to Default Configuration	Щелкните кнопку Restore, чтобы восстановить конфигурацию по умолчанию.	—
Restore to Factory Default Configuration	Щелкните кнопку Restore, чтобы восстановить заводскую конфигурацию по умолчанию. Примечание: Файловая система Linux будет восстановлена до состояния инициализации.	—

Откат



Элемент	Описание	По умолчанию
Save as a Rollbackable Archive	Создание точки сохранения вручную. Кроме того, система ежедневно автоматически создает точку сохранения, если конфигурация изменена.	—
Configuration Archive Files	Просмотр соответствующей информации о файлах архива конфигурации, включая имя, размер и время изменения.	—

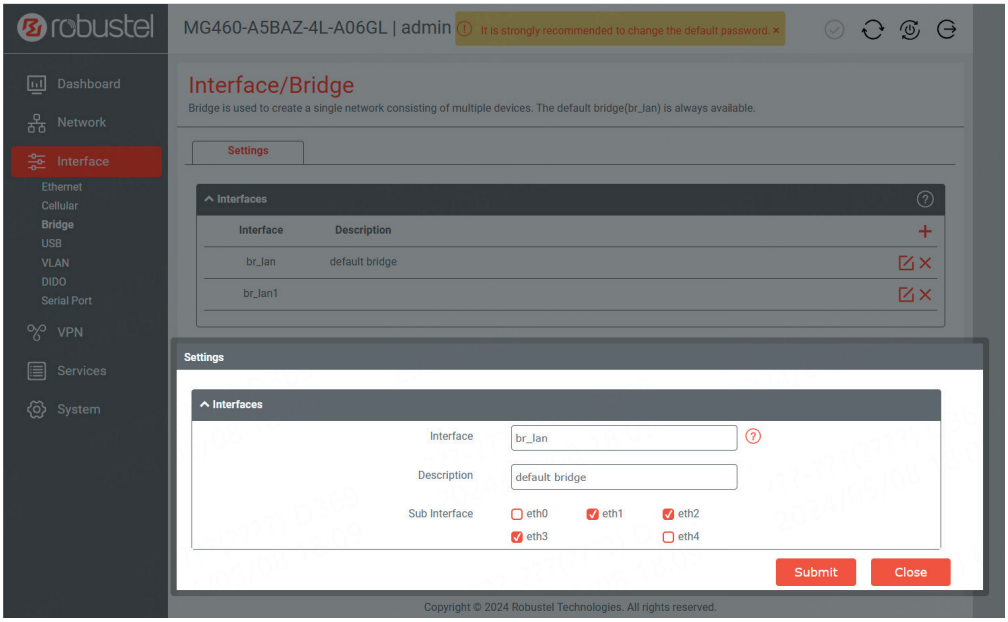
Глава 5. НАСТРОЙКИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ СТАНДАРТА IEC61162–460

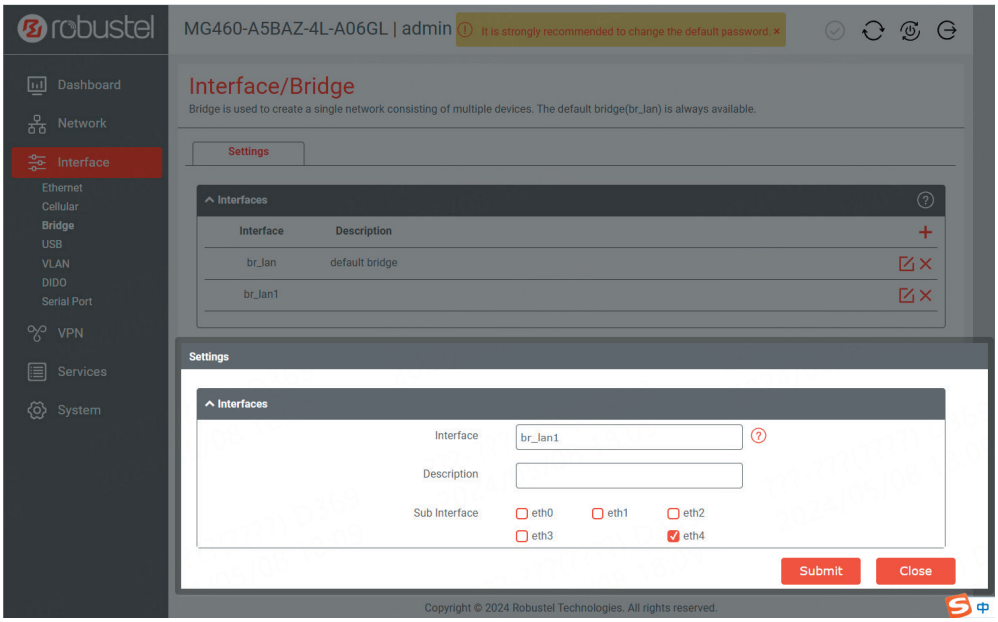
По умолчанию шлюз настроен в соответствии с требованиями стандарта IEC 61162–460. Пользователям не нужно выполнять сложные настройки. Однако, чтобы помочь пользователям в проверке настроек на соответствие требованиям IEC 61162–460, мы предоставляем перечень действий для настройки конфигурации в соответствии со стандартом IEC 61162–460.

1. Чтобы настроить WAN, пользователи могут зайти в меню и выбрать один из трех поддерживаемых типов соединений WAN. Пользователи могут настроить параметры WAN в соответствии с конкретными требованиями, чтобы обеспечить надежное подключение.

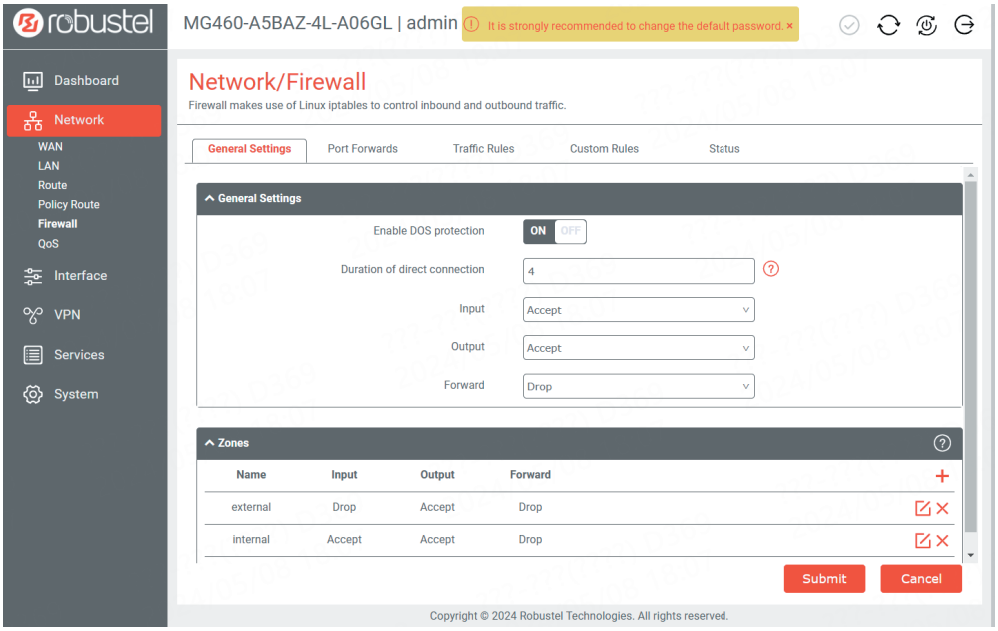
2. Настройте LAN для устройств сети 460 или DMZ. Например, настройте подключение к локальной сети, включающее ETH1, ETH2 и ETH3 для устройства сети 460, и другое подключение к локальной сети с ETH4 для DMZ. Каждое подключение должно иметь свой собственный IP-адрес, назначенный пользователем.


robustel
MG460-A5BAZ-4L-A06GL | admin
It is strongly recommended to change the default password.
Dashboard
Network
WAN
LAN
Route
Policy Route
Firewall
QoS
Interface
VPN
Services
System
Network/LAN
A Local Area Network (LAN) connects network devices together, such as Ethernet or Bridge, in a logical Layer-2 network. The default link(br_lan) is always available.
Link
Status
Settings
Name
Type
Description
Firewall Zone
LAN1
Bridge
default lan
internal
LAN2
Bridge
lan2
internal
Submit
Cancel
Copyright © 2024 Robustel Technologies. All rights reserved.

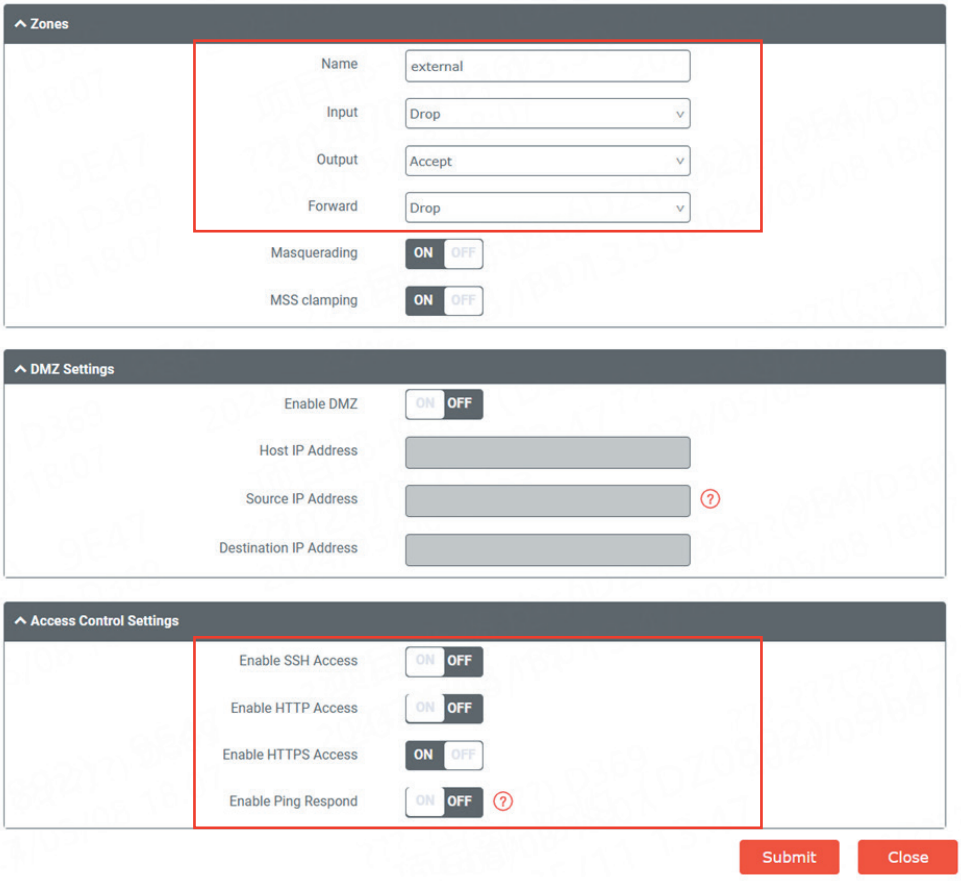

robustel
MG460-A5BAZ-4L-A06GL | admin
It is strongly recommended to change the default password.
Dashboard
Network
Interface
Ethernet
Cellular
Bridge
USB
VLAN
DIDO
Serial Port
VPN
Services
System
Interface/Bridge
Bridge is used to create a single network consisting of multiple devices. The default bridge(br_lan) is always available.
Settings
Interfaces
Interface
Description
br_lan
default bridge
br_lan1
Settings
Interfaces
Interface
br_lan
Description
default bridge
Sub Interface
eth0
eth1
eth2
eth3
eth4
Submit
Close
Copyright © 2024 Robustel Technologies. All rights reserved.


robustel
MG460-A5BAZ-4L-A06GL | admin
It is strongly recommended to change the default password.
Dashboard
Network
Interface
Ethernet
Cellular
Bridge
USB
VLAN
DIDO
Serial Port
VPN
Services
System
Interface/Bridge
Bridge is used to create a single network consisting of multiple devices. The default bridge(br_lan) is always available.
Settings
Interfaces
Interface
Description
br_lan
default bridge
br_lan1
Settings
Interfaces
Interface
br_lan1
Description
Sub Interface
eth0
eth1
eth2
eth3
eth4
Submit
Close
Copyright © 2024 Robustel Technologies. All rights reserved.

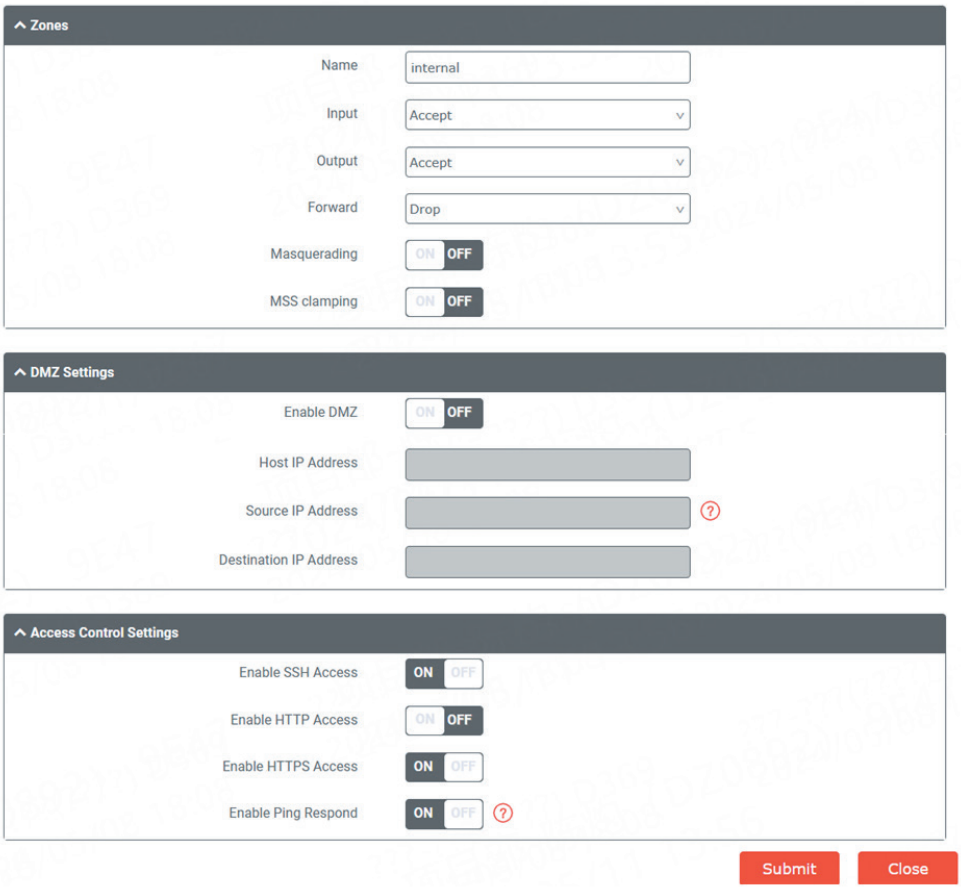
3. Настройте правило firewall. Убедитесь, что включена защита функция DOS protection. По умолчанию продолжительность прямого подключения составляет 4 часа, при необходимости ее можно изменить.



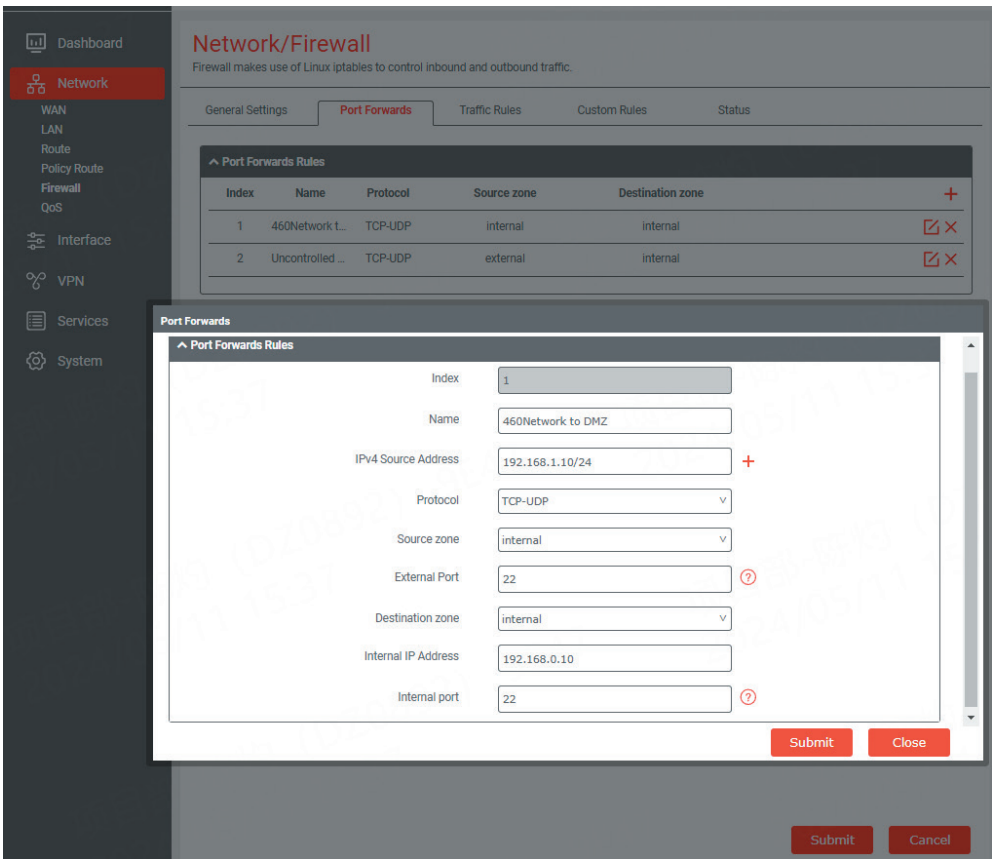
4. Установите правило firewall для внешней зоны. Input — drop, output — accept, forward — drop. Для настройки контроля доступа включите только HTTPS Access.



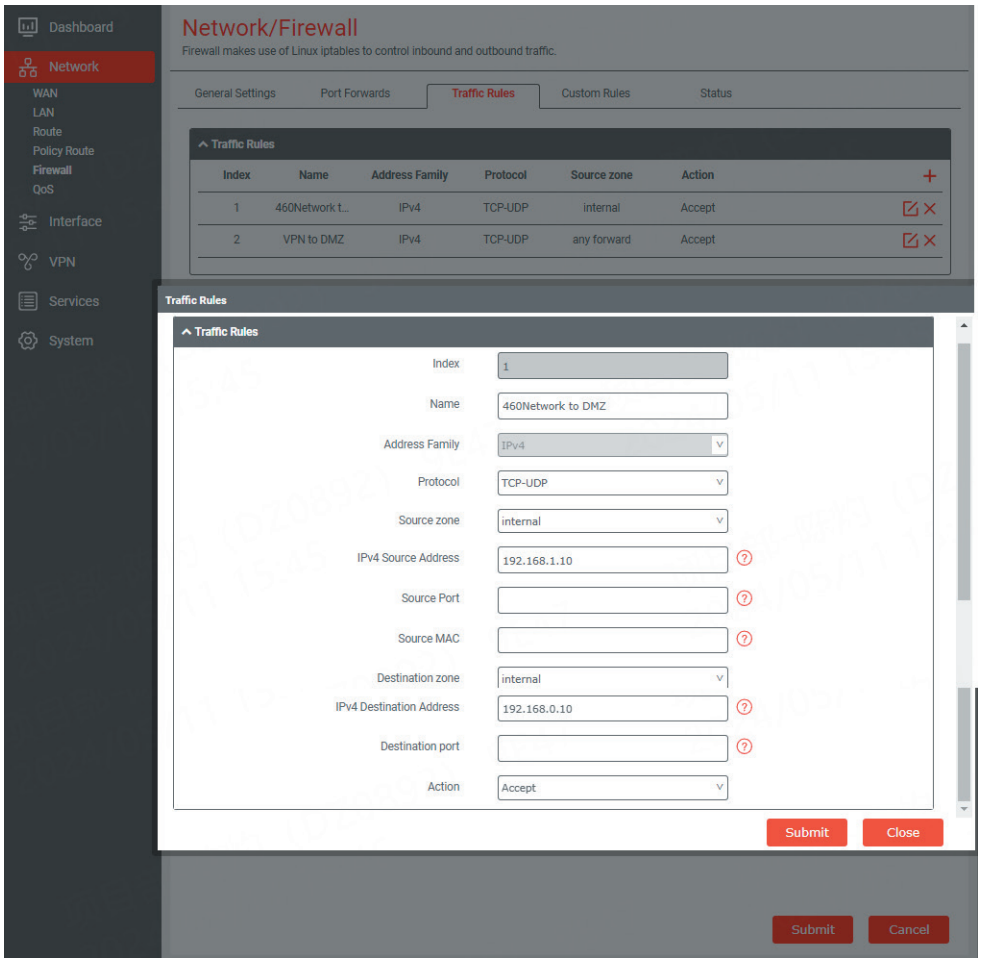
5. Установите правило firewall для внутренней зоны. Input — accept, output — accept, forward — drop. Для настройки контроля доступа включите доступ по SSH, HTTPS и Ping Response.



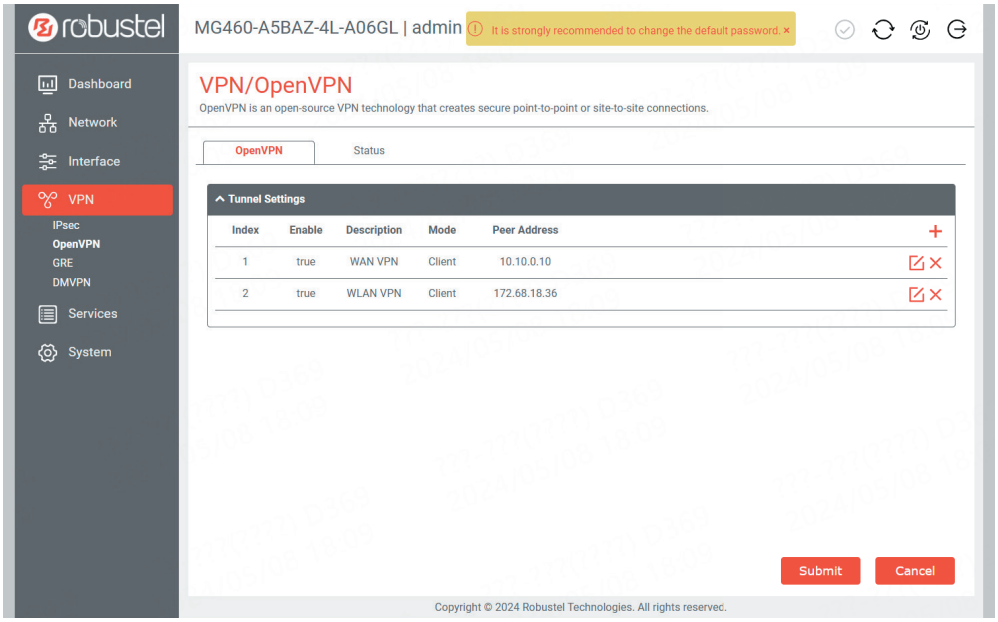
6. Если требуется, установите правило firewall для переадресации портов. Например, вот настройки для переадресации данных сети 460 на адрес сети DMZ.

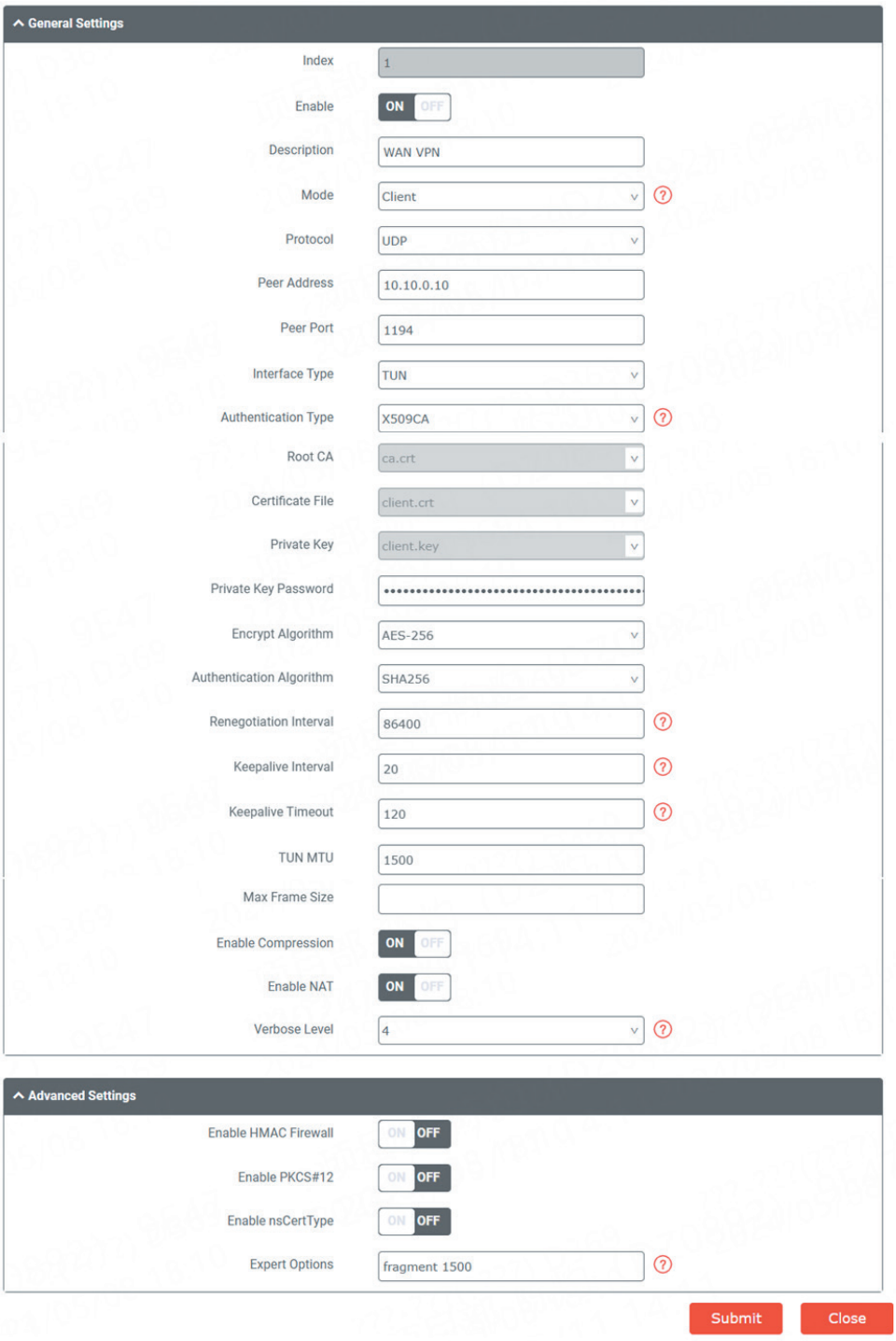


7. Если требуется, установите правило firewall для трафика. Например, вот правило трафика из сети 460 до адреса DMZ.

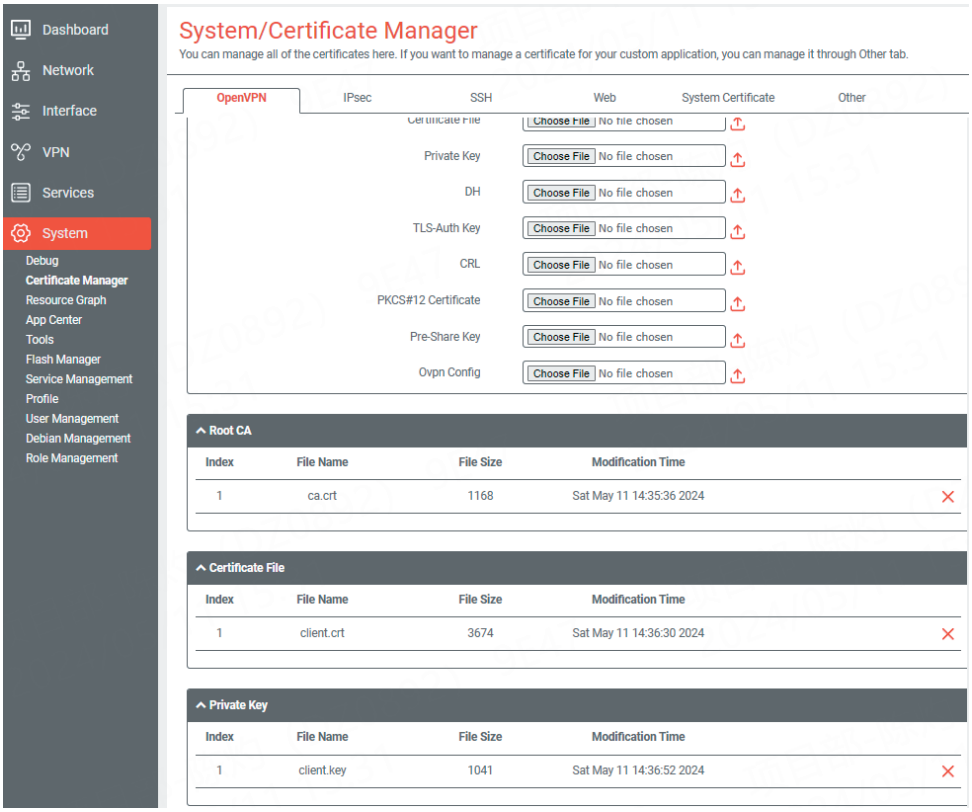


8. Установите VPN-соединение между сетью 460 и неконтролируемой сетью. Для этого необходимо установить правильный peer адрес (из неконтролируемой сети), импортировать сертификат X509CA, установить алгоритм шифрования AES256, алгоритм аутентификации SHA256.

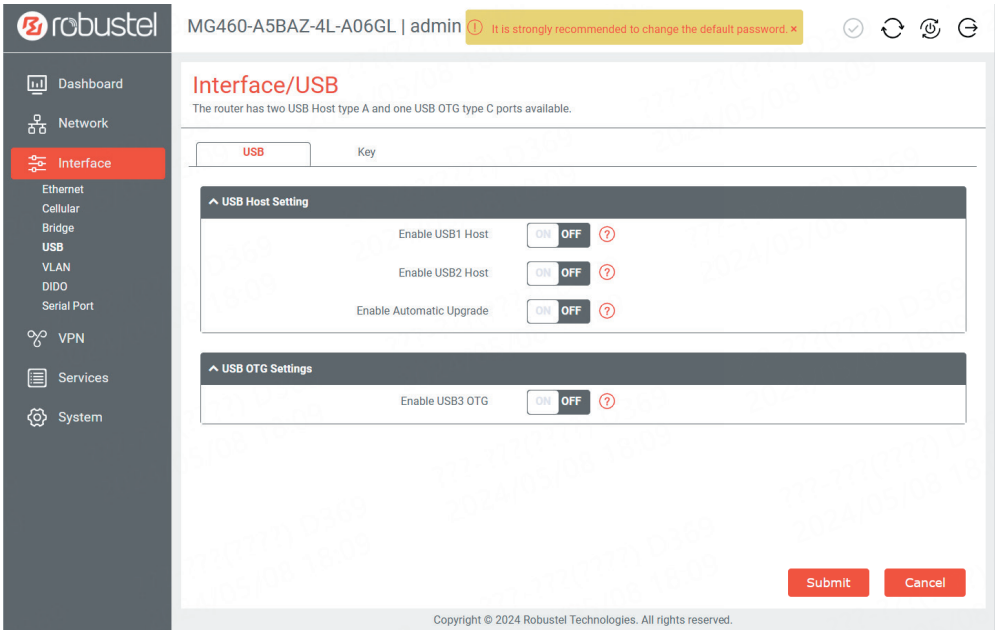



General Settings
Index
1
Enable
ON
OFF
Description
WAN VPN
Mode
Client
Protocol
UDP
Peer Address
10.10.0.10
Peer Port
1194
Interface Type
TUN
Authentication Type
X509CA
Root CA
ca.crt
Certificate File
client.crt
Private Key
client.key
Private Key Password
Encrypt Algorithm
AES-256
Authentication Algorithm
SHA256
Renegotiation Interval
86400
Keepalive Interval
20
Keepalive Timeout
120
TUN MTU
1500
Max Frame Size
Enable Compression
ON
OFF
Enable NAT
ON
OFF
Verbose Level
4
Advanced Settings
Enable HMAC Firewall
ON
OFF
Enable PKCS#12
ON
OFF
Enable nsCertType
ON
OFF
Expert Options
fragment 1500
Submit
Close

9. Загрузите сертификат OpenVP N.



10. Отключите USB-порты, оставьте USB-порты отключенными, когда они находятся в режиме ожидания.



Ниеншанц
Автоматика

«Ниеншанц-Автоматика» — это команда профессионалов, готовых поделиться опытом и наработками в сфере высоких технологий. У нас есть все для того, чтобы заказчик мог в короткие сроки реализовать свой проект: более 25 лет опыта, широкий ассортимент товаров и складских запасов, высококвалифицированные инженеры, индивидуальные условия. Мы постоянно растем и развиваемся, повышаем квалификацию и наращиваем список партнеров и поставщиков, чтобы предоставлять нашим клиентам самые современные технические решения.

НАША ЦЕЛЬ — ВАШИ УСПЕШНО РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

Санкт-Петербург
(812) 326-59-24
ipc@nnz.ru

Москва
(495) 980-64-06
msk@nnz.ru

Екатеринбург
(343) 311-90-07
ekb@nnz-ipc.ru

Новосибирск
(383) 330-05-18
nsk@nnz-ipc.ru