irzOS
Интерфейс командной строки

Содержание

1. Доступ в интерфейс командной строки (CLI)

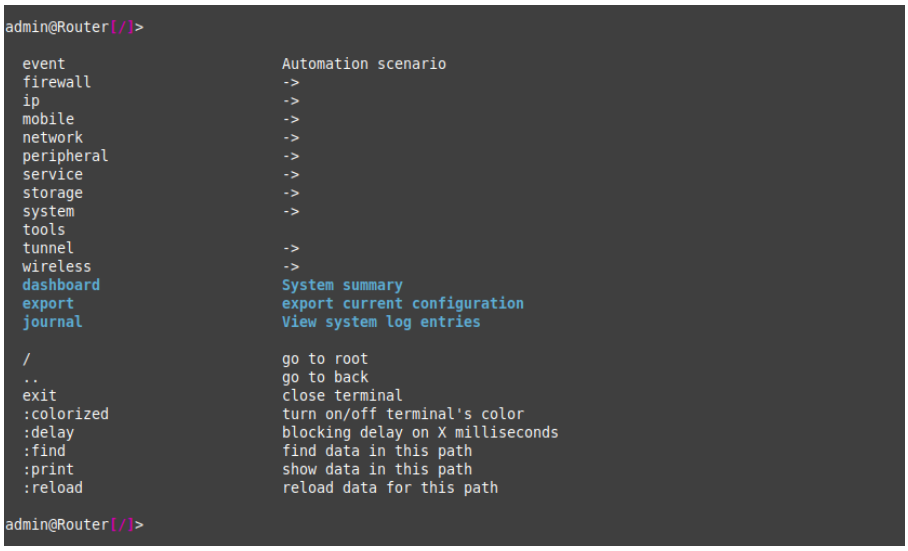
Доступ к интерфейсу командной строки (CLI) осуществляется по протоколу SSH. После успешной аутентификации пользователь получает доступ в CLI с правами, соответствующими учетной записи.

Процесс доступа:

1. Установить SSH-соединения с IP-адресом роутера (адрес роутера по умолчанию указан на наклейке на корпусе)
2. Пройти аутентификацию (указать пароль)
3. После этого устройство автоматически покажет интерфейс командной строки (cli)

```
user@desktop:~$ ssh admin@192.168.1.1
admin@192.168.1.1's password:
admin@Router[/]>
```

2. Навигация и управление



TAB - показать все разделы

? - показать все разделы с подсказками

.. - вернуться на один уровень выше

/ - вернуться в корневой раздел

dashboard - показать статусную информацию об устройстве

export - экспортировать текущую конфигурацию устройства. При вызове без аргументов в консоли будет показана текущая конфигурация полностью.

export ip - экспортировать конфигурацию раздела

export [TAB] **to-file=** экспортировать в файл

journal - системный лог. При вызове без аргументов в консоли будут показаны данные лога полностью.

journal [TAB] **filter=** показать строки, содержащие определенную информацию

journal [TAB] **last=** показать последние N строк

exit - закрыть терминал

colorized - включить/выключить цветовую схему

reload - обновить страницу

Зайти в конкретный раздел можно, перемещаясь последовательно по подразделам:

```
admin@iRZ-Router[/]>network
```

Ответ будет такой:

```
admin@iRZ-Router[/network]>
```

Также можно указать полный путь к разделу. Полный путь указывается последовательно, через пробел, без дополнительных символов, автодополнение по клавице TAB работает.

Например:

```
 network bridge
```

Ответ будет такой:

```
admin@iRZ-Router[/network bridge]>
```

Чтобы **просмотреть содержимое раздела**, нужно нажать **TAB** или **?**

```
admin@Router[/network bridge]>

  NAME       PORT   STP-VERSION
  bridge0    port1  none
             port2
             port3
             port4
             wifi1
  add
  apply
  clean
  export
  status
```

Добавить или удалить элементы

Чтобы добавить или удалить элементы из перечня нужно зайти в соответствующий раздел и написать имя добавляемого элемента (для удаления - со знаком минус)

Например:

Посмотреть список портов на bridge0

```
admin@iRZ-Router[/network bridge bridge0]>port
```

Ответ будет таким:

```
port1,port2,port3,port4
```

Добавить port 1 в список портов на bridge0:

```
admin@iRZ-Router[/network bridge bridge0]>port port1
```

Удалить port 1 из списка портов на bridge0:

```
admin@iRZ-Router[/network bridge bridge0]>port -port1
```

3. event

Раздел представляет собой инфраструктуру для автоматизации действий роутера в ответ на определенные изменения состояния системы или сети.

В отличие от простой модели «если-это-то-то», система построена на основе модульных, многоразовых компонентов. Это позволяет создавать сложные рабочие процессы автоматизации.

КОМАНДЫ

reorder	Изменить позицию объекта

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
description	Описание события
trigger	Подсистема-источник события (откуда пришло событие)
target	Объект-источник события **условия:** trigger = gpio trigger = gpi trigger = extra-gpi trigger = sms
value	Значение объекта для сравнения события **условия:** trigger = gpio trigger = gpi trigger = sms
action	CLI команда, выполняемая, если входящее событие соответствует конфигурации

4. firewall

4.1. connections

Данный раздел предоставляет оперативный мониторинг и управление активными сетевыми соединениями, проходящими через роутер. Являясь центральным компонентом системы безопасности роутера, система отслеживания соединений (Connection Tracker) поддерживает информацию о состоянии (stateful) каждого соединения, что позволяет принимать обоснованные решения о разрешении или блокировке трафика.

Раздел предоставляет наглядную информацию о том, какие внутренние устройства устанавливают соединения, с какими внешними IP-адресами и портами они взаимодействуют, а также о текущем состоянии этих соединений. Эта информация позволяет роутеру более эффективно применять правила межсетевого экрана и повышать уровень сетевой безопасности.

КОМАНДЫ

flush	Очистить таблицу conntrack

СВОЙСТВА

source	Адрес источника
destination	Адрес назначения

protocol	Протокол, инкапсулированный в IP
timeout	Интервал, через который сетевое соединение будет удалёно
tcp-state	Текущее состояние TCP соединения
mark	Метка пакета
pkts	Количество пакетов переданных через соединение (исходящих/входящих)
bytes	Количество байт переданных через соединение (исходящих/входящих)

4.2. defaults

В данном разделе определяются глобальные политики межсетевого экрана, действующие по умолчанию. Эти правила решают, что делать с любым сетевым пакетом, который не подошел ни под одно из более конкретных правил, созданных пользователем. Базовые политики имеют самый низкий приоритет и анализируются только после обработки всех остальных специфичных правил.

Конфигурация применяется к трем основным цепочкам:

- **INPUT:** Контролирует трафик, предназначенный для локальных процессов самого роутера, например, административный доступ (HTTPS, SSH), ответы ICMP или терминирование VPN-туннелей.
- **OUTPUT:** Контролирует трафик, генерируемый самим роутером, например, DNS-запросы, запросы NTP-клиента или трафик, инициированный утилитами мониторинга соединений.
- **FORWARD:** Контролирует транзитный трафик, проходящий через роутер между различными сетевыми интерфейсами или зонами, например, пересылку пакетов из зоны LAN в зону WAN.

СВОЙСТВА

input **значения:** accept, drop	Политика по умолчанию для входящего трафика
output **значения:** accept, drop	Политика по умолчанию для исходящего трафика
forward **значения:** accept, drop	Политика по умолчанию для пересылаемого (проходящего) трафика
drop-invalid **значения:** true, false	Откидывать неидентифицированные пакеты
syn-flood **значения:** true, false	Зашита от SYN Flood атак
syn-flood-rate	Допустимый порог количества TCP SYN пакетов в секунду **условия:** syn-flood = true
syn-flood-burst	Допустимый мгновенный всплеск количества TCP SYN пакетов **условия:** syn-flood = true
tcp-syncookies **значения:** true, false	Использовать TCP SYN cookies для противодействия TCP SYN flood
tcp-ecn **значения:** true, false	Использовать ECN (явное уведомление о перегруженности)

tcp-window-scaling **значения:** true, false	Масштабирование TCP окна
use-conntrack **значения:** true, false	Механизм отслеживания соединений (conntrack)
flow-offloading **значения:** true, false	Механизм разгрузки потока (Flow offloading)

4.3. filter

Раздел предназначен для настройки основных разрешающих и блокирующих правил, т.е.фильтрации трафика.

Этот раздел предназначен для настройки основного набора правил фильтрации пакетов. Эти пользовательские правила обеспечивают точный контроль над всем трафиком — как транзитным, так и адресованным непосредственно роутеру, и составляют основу политики сетевой безопасности.

Каждое правило состоит из определенных критериев соответствия — таких как зоны источника и назначения, IP-адреса, протоколы и порты — и заданного целевого действия (**ACCEPT**, **DROP** или **REJECT**). Межсетевой экран анализирует эти правила в последовательном порядке. Действие над пакетом определяется первым правилом, которому он соответствует, после чего дальнейшая обработка этого пакета прекращается.

Пакеты, которые не соответствуют ни одному правилу в этом списке, будут обработаны общими политиками, настроенными в подразделе «Defaults». Этот механизм позволяет создавать исключения из общей политики безопасности, разрешая работу определенных служб и соединений.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled **значения:** true, false	Отключить правило файрвола
chain **значения:** input, forward, output	Цепочка правил таблицы
src **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = output
src-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = input
dst-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика

protocol **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола
icmp-type **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
mark **пример:** 16, !453	Сравнение по метке пакета
action **значения:** accept, reject, drop	Действие над трафиком, попавшим под правило
policy **значения:** dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	Сопоставление для IPSec трафика
extra **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы (поддержка синтаксиса iptables)

4.4. mangle

Данный раздел позволяет создавать правила для изменения определенных атрибутов IP-пакетов до того, как они будут обработаны системами маршрутизации или фильтрации. Основная функция таблицы Mangle — это классификация и маркировка пакетов. Эти метки не разрешают и не блокируют трафик напрямую, а служат внутренними идентификаторами для других подсистем роутера.

Этот функционал необходим для реализации расширенных сетевых функций, таких как:

- **Маршрутизация на основе политик (PBR):** Направление маркированных пакетов через определенные WAN-интерфейсы или VPN-туннели в обход основной таблицы маршрутизации.
- **Качество обслуживания (QoS):** Приоритизация или ограничение полосы пропускания для потоков трафика на основе их меток.

Кроме того, правила Mangle могут использоваться для прямого изменения полей IP-заголовка, таких как DSCP (для классификации QoS) или TTL (Время жизни).

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled **значения:** true, false	Отключить правило файрвола

chain **значения:** prerouting, input, forward, output, postrouting	Цепочка правил таблицы
src **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = output chain = postrouting
src-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = input chain = prerouting
dst-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика
protocol **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола
icmp-type **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
mark **пример:** 16, !453	Сравнение по метке пакета
action **значения:** accept, dscp, mark, tcpmss, ttl	Действие над трафиком, попавшим под правило **условия:** chain = input
set-mark **минимум:** 0, **максимум:** 4294967295	Метка, которую следует установить для пакета **условия:** action = mark
set-dscp **значения:** cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, be, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, ef	Указать DiffServ класс в поле DSCP для приоретизации трафика **условия:** action = dscp
set-mss **значения:** clamp-mss-to-pmtu	Установить значение MSS в пакете TCP SYN **условия:** action = tcpmss
set-ttl **пример:** 1, 255, +1, -1	Изменить значение TTL в пакете **условия:** action = ttl
policy **значения:** dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	Сопоставление для IPSec трафика
extra **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы

4.5. nat

Данный раздел используется для настройки правил трансляции сетевых адресов (Network Address Translation, NAT). Эти правила модифицируют IP-адрес и/или порт источника и назначения в пакетах, проходящих через роутер. NAT является основной функцией для управления трафиком между приватными и публичными сетями.

Доступны следующие действия:

- **ACCEPT:** Явно отключает NAT для трафика, соответствующего правилу. Используется для создания исключений — например, чтобы предотвратить трансляцию адресов для трафика, направленного в определенный VPN-туннель или другую приватную сеть.
- **SNAT:** Транслирует IP-адрес источника в конкретный, статически заданный IP-адрес. Это действие обычно используется, когда WAN-интерфейс роутера имеет статический публичный IP-адрес.
- **Masquerade:** Динамически транслирует IP-адрес источника в текущий IP-адрес исходящего интерфейса. Это стандартное и рекомендуемое действие для интерфейсов с динамическими IP-адресами, например, для сотовых (LTE) или DHCP-подключений.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled **значения:** true, false	Отключить правило файрвола
chain **значения:** prerouting, postrouting, output	Цепочка правил таблицы
src **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = postrouting
src-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = prerouting
dst-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика
protocol **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола

icmp-type **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
mark **пример:** 16, !453	Сравнение по метке пакета
action	Действие над трафиком, попавшим под правило **условия:** chain = output chain = prerouting chain = postrouting
nat-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	Преобразовать адрес попавшего под правила пакета **условия:** chain = output && action = dnat chain = prerouting && action = dnat chain = postrouting && action = snat
redirect-port **пример:** 80, !80	Транслировать попавшие под правило пакеты на указаный порт **условия:** chain = output && action = redirect chain = prerouting && action = redirect
policy **значения:** dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	Сопоставление для IPSec трафика
extra **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы

4.6. raw

В этом разделе настраиваются правила в таблице Raw — самой первой точке обработки на пути следования пакетов в межсетевом экране. Правила здесь оперируют «сырыми» пакетами до того, как они передаются в систему отслеживания соединений с состоянием (conntrack).

Основное назначение этой таблицы — находить определенные потоки трафика и применять к ним действие **NOTRACK**, которое указывает межсетевому экрану полностью пропустить инспекцию этих пакетов с отслеживанием состояния. Это может быть необходимо для:

- **Сценариев с высокой производительностью:** Чтобы снизить нагрузку на процессор и память роутера при обработке чрезвычайно высокой интенсивности трафика без отслеживания состояния.
- **Совместимости с протоколами:** Для обработки протоколов, которые по своей природе несовместимы с инспекцией состояний или с трансляцией сетевых адресов (NAT).

Пакеты, помеченные *NOTRACK*, не обрабатываются механизмом межсетевого экрана, отслеживающим состояния. Следовательно, к ним не могут применяться правила, основанные на состоянии (например, *RELATED*, *ESTABLISHED*), и они несовместимы со стандартным функционалом NAT. Эту функцию следует использовать с четким пониманием ее последствий для безопасности.

КОМАНДЫ

reset-counters	Сброс счётчиков

reorder	Изменить позицию объекта

СВОЙСТВА

disabled **значения:** true, false	Отключить правило файрвола
chain **значения:** output, prerouting	Цепочка правил таблицы
src **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = output
src-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = prerouting
dst-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика
protocol **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола
icmp-type **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
action **значения:** accept, drop, notrack	Действие над трафиком, попавшим под правило
extra **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы

4.7. zone

Данный раздел предназначен для создания и определения зон межсетевого экрана. Зоны — это логические контейнеры для классификации источников и назначений трафика, которые служат основными элементами для построения политик безопасности. Принадлежность к зоне определяется ее типом конфигурации:

- **Зона на основе интерфейсов:** Связывает зону с одним или несколькими сетевыми интерфейсами (например, *eth0*, *br-lan*, *tun0*). Весь трафик, входящий или исходящий через выбранный интерфейс, считается частью этой зоны. Это стандартный метод для сегментации физических или логических сетевых сегментов.

- **Зона на основе адресов:** Определяет зону по списку IP-адресов, подсетей в нотации CIDR или диапазонов IP-адресов. Трафик считается частью этой зоны, если его IP-адрес источника или назначения соответствует записи в списке, независимо от физического интерфейса, через который он проходит. Это позволяет создавать политики, независимые от топологии сети.

После создания эти зоны могут использоваться в качестве источника и назначения для построения политики безопасности.

СВОЙСТВА

type **значения:** interface, address	Тип набора
entry	Участники набора **условия:** type = interface type = address

5. ip

5.1. arp

Данный раздел предоставляет интерфейс для просмотра и управления таблицей протокола разрешения адресов (Address Resolution Protocol, ARP) роутера. Протокол ARP является ключевым механизмом для сопоставления адресов 3-го уровня (IP) с адресами 2-го уровня (MAC) в пределах одного локального сетевого сегмента.

Страница выполняет две основные функции:

1. Просмотр ARP-кэша: Отображает текущий, динамически заполняемый ARP-кэш, в котором содержатся все активные сопоставления IP- и MAC-адресов, автоматически определённые роутером. Для каждой записи предоставляется информация о ее состоянии, включая IP- и MAC-адрес, соответствующий сетевой интерфейс и время до истечения срока действия записи.

2. Управление статическими ARP-записями: Основная функция этого раздела — создание статических ARP-записей. Статическая запись, или «статическая привязка ARP», формирует постоянное, неистекающее сопоставление между IP-адресом и конкретным MAC-адресом. Это важная функция для обеспечения безопасности и управления сетью, используемая для:

    - Повышения безопасности: Предотвращения атак типа «ARP-спуфинг», в ходе которых злоумышленник пытается выдать себя за легитимное сетевое устройство, связывая свой MAC-адрес с IP-адресом жертвы.

    - Обеспечения стабильности сети: Гарантирования постоянной доступности критически важных устройств (таких как серверы, шлюзы или IP-камеры) по неизменной паре IP-MAC, что исключает потенциальные проблемы с подключением, вызванные истечением записей в ARP-кэше или неверным динамическим разрешением.

Настройка статической записи гарантирует, что для указанного IP-адреса роутер всегда будет доверять только заданному MAC-адресу, игнорируя любые конфликтующие ARP-объявления для этого IP.

КОМАНДЫ

flush	Очистить таблицу ARP записей

СВОЙСТВА

ip-address **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	IP адрес
macaddr **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
interface **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tp-v3, /tunnel atunnel, /defaults server **пример:** bridge0	Интерфейс

5.2. interface

Этот раздел предназначен для настройки и управления логическими интерфейсами 3-го уровня (L3) устройства. Каждый интерфейс представляет собой логическую сущность, которая связывает IP-адрес и соответствующие параметры L3 с нижележащим сетевым устройством, формируя основу для всех политик маршрутизации, межсетевого экрана и сервисов.

Процесс настройки включает в себя установку общих параметров, применимых ко всем интерфейсам, таких как административное состояние, метрика маршрута и настройки DNS.

Кроме того, параметры, специфичные для протокола, определяют метод настройки IP-адреса:

- **Статический (Static):** Для ручного назначения фиксированного адреса IPv4 или IPv6 и подсети.
- **DHCP-клиент (DHCP Client):** Для динамического получения IP-адреса от вышестоящего DHCP-сервера, с опциями для идентификации клиента.
- **PPPoE:** Для установки сессий с аутентификацией по протоколу Point-to-Point Protocol over Ethernet, включая настройку учетных данных и параметров, специфичных для данного типа соединения.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
metric **минимум:** 0, **максимум:** 8388608	Значение метрики маршрута
ip-address	IP адрес интерфейса **условия:** type = static
defaultroute **значения:** true, false	Добавить маршрут по умолчанию через этот интерфейс **условия:** type != static
gateway **пример:** 192.168.1.1	Адрес шлюза для маршрута по-умолчанию **условия:** type = static
peer-dns **значения:** true, false	Использовать полученные DNS серверы для разрешения имён **условия:** type = pppoe type = dhcp

pppoe-username	Имя пользователя для PPPoE аутентификации **условия:** type = pppoe
pppoe-password	Пароль для PPPoE аутентификации **условия:** type = pppoe
pppoe-ac	Имя PPPoE Access Concentrator для подключения **условия:** type = pppoe
pppoe-service	Клиентская служба PPPoE, поддерживаемся AC **условия:** type = pppoe
pppoe-option **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, padi-attempts, padi-timeout, mru, mtu	Дополнительные опции протокола PPP **условия:** type = pppoe
debug **значения:** true, false	Режим подробного логгирования **условия:** type = pppoe
hostname	Переопределить hostname клиента в DHCP запросе **условия:** type = dhcp
dhcp-clientid	Уникальный Client ID (DHCP option 61) **условия:** type = dhcp
dhcp-vendorid	Уникальный Vendor ID (DHCP option 60) **условия:** type = dhcp

5.3. route

5.3.1. list

В данном разделе отображается список всех статически настроенных маршрутов. Так же раздел служит основным интерфейсом для управления ими. Здесь вы можете создавать новые статические записи, изменять существующие или удалять их по мере необходимости.

Каждый маршрут, настроенный в этом списке, является постоянной инструкцией, которая добавляется в основную таблицу маршрутизации. Это обеспечивает точный и постоянный контроль над путями трафика, в отличие от маршрутов, полученных динамически или созданных автоматически. Данный список является представлением всех вручную заданных политик маршрутизации на устройстве.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
dst-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес сети или хост к которому нужно указать маршрут
gateway **пример:** 192.168.1.1	Шлюз для доступа к сети или адресу назначения **условия:** type = unicast

metric **минимум:** 0, **максимум:** 8388608	Метрика маршрута, определяющая его предпочтительность
table **значения:** /ip route table, main	Таблица маршрутизации, для которой предназначен маршрут
src-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес для отправки трафика при использовании этого маршрута
type **значения:** unicast, unreachable, prohibit, blackhole	Тип маршрута
interface **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tp-v3, /tunnel atunnel, /defaults server **пример:** bridge0	Интерфейс для отправки трафика при использовании этого маршрута **условия:** type = unicast

5.3.2. rule

Раздел является центром механизма маршрутизации на основе политик (Policy-Based Routing, PBR). Он позволяет создавать сложные политики управления трафиком путем определения правил, которые классифицируют трафик на основе заданных атрибутов.

В отличие от стандартной маршрутизации, которая, как правило, учитывает только адрес назначения, правила PBR могут анализировать трафик по более широкому набору критериев, таких как IP-адрес источника, входящий интерфейс или метка межсетевого экрана (fwmark). Когда пакет соответствует условиям правила, он направляется на поиск маршрута в указанную таблицу маршрутизации, что переопределяет стандартное поведение системной маршрутизации.

Данный функционал необходим для реализации сложных сетевых сценариев, таких как балансировка нагрузки между несколькими WAN-каналами, маршрутизация трафика из определенных VLAN через VPN-туннель или изоляция гостевого сетевого трафика от корпоративного. Правила обрабатываются в порядке назначенного им приоритета, что обеспечивает точный контроль над логикой принятия решений о маршрутизации.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
interface **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tp-v3, /tunnel atunnel, /defaults server, any **пример:** bridge0	Сопоставление по интерфейсу источника пакета
src-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Сопоставление по адресу источника пакета
dst-addr **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Сопоставление по адресу назначения пакета
mark **минимум:** 0, **максимум:** 4294967295	Сопоставление по conntrack метке пакета
table **значения:** /ip route table	Таблица с маршрутами для сопоставленного пакета

action **значения:** prohibit, unreachable, blackhole, throw	Тип предпринимаемого действия при совпадении правила
priority **минимум:** 1, **максимум:** 9999999	Приоритет правила в порядке сопоставления

5.3.3. table

Данный раздел предназначен для определения и управления пользовательскими таблицами маршрутизации. Эти таблицы являются ключевым компонентом для реализации сложных сценариев маршрутизации, в особенности — маршрутизации на основе политик (Policy-Based Routing, PBR), которая позволяет принимать различные решения о маршрутизации на основе характеристик трафика.

Хотя система использует несколько таблиц по умолчанию (main, local и др.), данный интерфейс позволяет создавать дополнительные, именованные таблицы маршрутизации. Каждая новая таблица функционирует как независимое пространство имен для маршрутных записей, что дает возможность создавать отдельные политики маршрутизации для разных типов трафика.

Непосредственное наполнение этих таблиц статическими маршрутами осуществляется в разделе **IP/Route/List**, в то время как логика, направляющая определенный трафик на поиск маршрута в этих пользовательских таблицах, настраивается в разделе **IP/Rules**.

СВОЙСТВА

number **минимум:** 16384, **максимум:** 99999	Уникальный номер таблицы маршрутизации

6. mobile

6.1. apn

Раздел предназначен для работы с SIM-картами виртуальных операторов.

Виртуальные операторы используют сотовые сети базовых операторов (Мегафон, МТС, Билайн,Теле2). Для подключения к каждой из базовых сетей виртуальному оператору может потребоваться отдельное значение APN и код MCCMNC.

Для доступа в Интернет через современные сотовые сети базовых операторов явное указание APN, как правило, не требуется.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
mccmnc **пример:** 46000	PLMN код оператора (MCC and MNC)
apn **пример:** bridge0, vpn-client1, user_1@example.com	APN или имя VPDN
username **макс. длина:** 39 **пример:** bridge0, vpn-client1, user_1@example.com	Имя пользователя для аутентификации

password	Пароль пользователя для аутентификации
auth **значения:** any, pap, chap	Протокол аутентификации
mode **значения:** auto, /defaults modem_modes	Технология передачи данных
roaming **значения:** allowed, discard, only	Политика работы в роуминг сетях
slot **значения:** any, /mobile slot	Применить профиль к слоту SIM карты
pincode	PIN-код SIM карты **условия:** slot != any

6.2. modem

Этот раздел является основным центром управления для настройки сотового модема роутера и его подключения к интернету. Он предоставляет набор инструментов для управления всеми аспектами: от базового подключения до расширенных политик отказоустойчивости и выбора сети.

Настройки в этом разделе позволяют:

- **Конфигурировать параметры маршрутизации:** Определять, как сотовое соединение будет интегрировано в таблицу маршрутизации роутера. Вы можете управлять его приоритетом с помощью поля *Metric* и назначать его в качестве Маршрута по умолчанию.
- **Управлять отказоустойчивостью SIM-карт:** Для моделей, оснащенных модемом с поддержкой двух SIM-карт, этот раздел предоставляет надежные инструменты для обеспечения высокой доступности. Вы можете определить *Основную SIM-карту* и резервную, а также настроить *Интервал возврата к основной*, чтобы автоматически переключаться обратно на предпочтительную SIM-карту, как только она снова станет доступной.
- **Производить тонкую настройку надежности соединения:** Вы можете установить *Таймаут подключения*, чтобы модем выполнил перезагрузку по питанию и повторную попытку подключения, если ему не удается зарегистрироваться в сети в течение указанного периода.
- **Управлять регистрацией в сети:** Для сложных сценариев вы можете вручную выбрать *Определенные диапазоны (Bands)*, чтобы принудительно заставить модем использовать только определенные частоты, или использовать *Принудительный выбор MCCMNC*, чтобы зафиксировать устройство в сети конкретного оператора. Это особенно полезно для частных сетей LTE или для повышения стабильности соединения в зонах с перекрытием сетей.

Обратите внимание, что доступность определенных функций, таких как управление несколькими SIM-картами (*Primary SIM*, *Return to Primary*) и выбор *Specific Bands*, зависит от конкретной модели роутера, установленной в роутере. На странице также отображается ключевая информация о состоянии активного модемного соединения в реальном времени.

КОМАНДЫ

reset	Перезапуск модема со сбросом питания

СВОЙСТВА

disabled **значения:** true, false	Не выполнять подключение через модем

modem-sim-slot **значения:** $_available-sim-slots	Слоты SIM карт, с которыми модем может работать
modem-primary-sim **значения:** $modem-sim-slot	Слот основной SIM карты, на которой будет стремиться работать модем
modem-primary-sim-timeout	Таймер (сек) спустя который модем переключится на основную SIM карту с резервной
modem-connect-timeout **минимум:** 300	Таймер (сек) в течении которого пытаться установить соединение через текущую SIM карту
modem-band **значения:** $_available-bands	Частоты, на которых будеть пытаться работать модем, если выбрано
protocol **значения:** auto, ppp	Протокол дозвона модема
metric **минимум:** 101, **максимум:** 900	Метрика интерфейса модема
defaultroute **значения:** true, false	Добавить маршрут по умолчанию через этот интерфейс
peerdns **значения:** true, false	Использовать полученные DNS серверы для разрешения имён
mtu **минимум:** 400, **максимум:** 1500	MTU интерфейса

6.3. sms

Данный раздел предоставляет интерфейс для отправки и получения сообщений SMS непосредственно через сотовый модуль роутера.

Чтение SMS

Интерфейс отображает таблицу последних полученных SMS-сообщений. Этот список действует как циклический журнал, храня до 10 последних сообщений. При поступлении нового SMS, если журнал заполнен, самое старое сообщение автоматически удаляется, чтобы освободить место для нового.

Отправка SMS

Инструмент отправки позволяет создавать и отправлять SMS-сообщения на любой действительный номер телефона. Для успешной отправки сообщения должны быть выполнены следующие условия:

- На установленной SIM-карте должна быть активна услуга SMS и иметься достаточный баланс на счете.
- Роутер должен быть успешно зарегистрирован в сети оператора (т.е. находиться в зоне покрытия).

КОМАНДЫ

send-sms	Отправить SMS на произвольный номер phone-number - Номер телефона (обязательно) message - Текст SMS сообщения (обязательно) modem - Отправить SMS сообщение с определённого модема

СВОЙСТВА

from	Имя или номер отправителя SMS
text	Текст SMS сообщения
sent	Время отправки сообщения SMS центром
received	Время получения SMS сообщения на устройство

7. network

7.1. bridge

Раздел используется для создания и управления программно-определяемыми мостами 2-го уровня (L2). Сетевой мост (bridge) фактически функционирует как виртуальный коммутатор, объединяя несколько физических или логических сетевых интерфейсов (например, Ethernet-порты, VLAN-подинтерфейсы) в единый широковещательный домен.

Помимо базового объединения интерфейсов, данный раздел предоставляет набор расширенных функций управления 2-м уровнем:

- Протокол Spanning Tree (STP): Полная настройка протокола STP/RSTP для предотвращения образования петель в физически резервированных топологиях. Включает детальное управление приоритетом моста, состоянием портов и таймингами протокола для обеспечения стабильной и беспетлевой работы сети.
- IGMP Snooping: Функционал для оптимизации доставки многоадресного (multicast) трафика. При включении этой опции мост анализирует IGMP-сообщения и интеллектуально пересылает multicast-потоки только на те порты, которые их запросили, что значительно снижает избыточную сетевую нагрузку и повышает эффективность.
- Настройка производительности: Контроль над низкоуровневыми параметрами, такими как MTU и длина очереди передачи, для оптимизации производительности под конкретные сценарии использования.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
macaddr **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
tx-queue-len	Максимальное количество пакетов в очереди интерфейса
port **значения:** /network device, /network ethernet, /wireless network, /tunnel	Участники сетевого моста
vlan-default-pvid **минимум:** 1, **максимум:** 4095	Port Vlan ID, который будет присвоен не тэгированным пакетам переданным в этот порт **условия:** vlan-filtering = true
igmp-snooping **значения:** true, false	Отправлять мультикаст трафик только получателям, подключившимся к мультикаст группе
igmp-mc-querier **значения:** true, false	Предотвращение дублирования мультикаст трафика от нескольких маршрутизаторов **условия:** igmp-snooping = true

igmp-query-interval	Интервал (сек) между отправкой Querry сообщений **условия:** igmp-snooping = true
igmp-query-resp-interval	Время ожидания ответа от хоста на Querry сообщения **условия:** igmp-snooping = true
igmp-hash-max	Размер hash таблицы IGMP записей **условия:** igmp-snooping = true
igmp-robustness	Количество Querry без ответа, после отправки которых удалится IGMP запись **условия:** igmp-snooping = true
stp-version **значения:** none, rstp, stp	Выбор спецификации STP протокола
stp-bpdu-guard **значения:** $port	Выключить порт при получении BPDU **условия:** stp-version != none
stp-treeprio **минимум:** 1, **максимум:** 15	Приоритет узла внутри дерева **условия:** stp-version != none
stp-maxage **минимум:** 6, **максимум:** 40	Считать что связь с Root Bridge потеряна, если от него не получено BPDU за этот интервал **условия:** stp-version != none
stp-fdelay **минимум:** 6, **максимум:** 40	Время ожидания перехода порта из одного состояния в другое **условия:** stp-version != none
stp-maxhops **минимум:** 6, **максимум:** 40	Максимальное число прыжков до любого коммутатора **условия:** stp-version != none
stp-hello **минимум:** 1, **максимум:** 10	Интервал отправки BPDU сообщений корневым коммутатором **условия:** stp-version != none
stp-ageing **минимум:** 10, **максимум:** 1000000	Время нахождения MAC-адреса в FDB от получения последнего пакета с этого адреса **условия:** stp-version != none
stp-txholdcount **минимум:** 1, **максимум:** 10	Максимальное число отправляемых BPDU в секунду **условия:** stp-version != none

7.2. device

Раздел отвечает за низкоуровневое управление объектами сетевых устройств 2-го уровня (L2). В отличие от физических аппаратных портов (например, eth0, eth1), устройства, управляемые здесь, часто являются виртуальными или логическими сущностями, которые позволяют реализовать расширенные сетевые конфигурации. Это уровень, на котором создаются «строительные блоки» для сетевой топологии перед их использованием в конфигурациях более высокого уровня.

После того как логическое устройство определено здесь (со своим MAC-адресом, MTU и т.д.), оно может быть добавлено в сетевой мост (в разделе Network / Bridge) для коммутации на L2-уровне или настроено с IP-адресом (в разделе IP / Interface) для работы на 3-м уровне. Этот раздел предоставляет прямой контроль над сущностями L2, которые лежат в основе всего сетевого стека.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
type **значения:** vlan	Тип устройства
macaddr **пример:** FE:FF:FF:FF:FF:FF	MAC адрес устройства **условия:** type != vlan
mtu **минимум:** 70, **максимум:** 65535	MTU интерфейса
tx-queue-len	Максимальное количество пакетов в очереди интерфейса
device **значения:** /network ethernet, /tunnel	Создать новое устройство поверх другого устройства
vid **минимум:** 6, **максимум:** 4094	Идентификатор VLAN, которым тегируются кадры

7.3. ethernet

Раздел предоставляет прямой контроль над параметрами физического (L1) и канального (L2) уровней аппаратных Ethernet-портов роутера. Эти настройки являются основополагающими, поскольку они определяют физические рабочие параметры порта до его использования в любых логических конфигурациях более высокого уровня, таких как добавление в сетевой мост или назначение IP-интерфейсу.

Данный интерфейс позволяет выполнять тонкую настройку поведения портов для обеспечения совместимости с подключенными устройствами и оптимизации производительности сети. Ключевые настройки включают ручную установку **скорости и режима дуплекса** для решения проблем автосогласования, изменение **MTU** для соответствия специфическим требованиям сети, а также включение **неизбирательного режима (promiscuous mode)** для расширенного анализа и диагностики сетевого трафика.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
macaddr **пример:** FE:FF:FF:FF:FF:FF	MAC адрес порта
mtu **минимум:** 70, **максимум:** 1500	MTU (байт) ethernet порта
promisc **значения:** true, false	Порт будет принимать все пакеты, независимо от того, кому они адресованы
speed **значения:** /defaults ether_port_speed	Скорость ethernet порта
duplex **значения:** half, full	Могут ли данные передаваться одновременно в обе стороны **условия:** speed = auto

7.4. fdb

Раздел отображает таблицу MAC-адресов, обнаруженных сетевым мостом на своих портах. Эта таблица является ключевым компонентом коммутации на 2-м уровне (L2), поскольку она содержит сопоставления между MAC-адресами устройств и конкретными портами моста, к которым они подключены.

Мост автоматически добавляет в таблицу MAC-адрес каждого устройства, от которого получает трафик. Благодаря этой таблице, мост направляет трафик только на тот порт, где находится получатель, вместо того чтобы рассылать его на все порты (flooding).

Данный раздел, доступный только для чтения, является диагностическим инструментом для поиска неисправностей на L2-уровне, проверки топологии сети и определения, к какому порту подключено конкретное устройство.

СВОЙСТВА

mac	MAC адрес сетевого устройства
device	L2 интерфейс, ассоциированный с этим MAC адресом
age	Как давно была добавлена запись в FDB таблицу
type	Является ли сетевое устройство внешним или самим интерфейсом

7.5. qos

7.5.1. filter

Данный раздел предназначен для определения правил классификации, которые распределяют сетевой трафик для дальнейшей обработки системой Quality of Service (QoS). На этом этапе определяется, какой именно трафик получит приоритет.

Система обрабатывает набор классификаторов в соответствии с их приоритетом. Каждый классификатор проверяет пакеты на соответствие определенным критериям, таким как метка межсетевого экрана (*fwmark*), поля в IP-заголовке (с помощью фильтра *U32*) или другие атрибуты.

Как только пакет соответствует правилу классификатора, он направляется в определенную очередь для дальнейшей обработки планировщиком. Создавая точные правила классификации, можно эффективно разделить трафик по типам (например, VoIP, видео, файловые загрузки) и применить к каждому из них свой уровень обслуживания.

СВОЙСТВА

interface **значения:** /ip interface, /mobile modem	Имя интерфейса, к которому применяется очередь
prio	Приоритет классификатора, фильтр с меньшим приоритетом проверяется раньше
handle **минимум:** 0, **максимум:** 4294967295	Сопоставление по conntrack метке пакета
queue **значения:** /network qos queue	Направить классифицированный трафик в этот класс
band **значения:** 1, 2, 3	Направлять классифицированный трафик в эту полосу очереди типа prio

u32-ip-filter **значения:** dst, dport, src, sport, protocol, dscp, icmp_code, icmp_type	Классификация IP пакета по совпадению битовых значений
u32 **пример:** 0x00/0xff, 0x00/0xff at 0	Классификация IP пакета по 32-битному значению и маске с произвольным смещением

7.5.2. queue

Данный раздел предназначен для определения и управления дисциплинами очередей, которые обрабатывают трафик, классифицированный фильтрами QoS. Здесь выбирается алгоритм, который будет контролировать распределение полосы пропускания, приоритизацию и управление перегрузками в вашей сети.

Выбор дисциплины очереди является основой для поведения политики QoS. Доступны следующие типы:

- **Fair (Справедливая):** Простая, бесклассовая дисциплина, обеспечивающая справедливое распределение полосы пропускания между активными потоками данных. Эффективно снижает задержки (bufferbloat) без сложной настройки.
- **FIFO (Первым пришел — первым вышел):** Самая базовая бесклассовая очередь. Пакеты обрабатываются строго в порядке их поступления, без какой-либо приоритизации.
- **HTB (Hierarchical Token Bucket):** Мощная, классовая дисциплина для сложных сценариев. Позволяет создавать иерархию классов трафика, гарантировать и ограничивать полосу пропускания, а также разрешать классам заимствовать неиспользуемую полосу у других.
- **PRIO (Приоритетная):** Классовая дисциплина, которая разделяет трафик на фиксированное количество полос по приоритету. Обеспечивает строгую приоритизацию (полосы с более высоким приоритетом всегда обслуживаются первыми), но не выполняет ограничение скорости (шейпинг).
- **RED (Random Early Detection):** Бесклассовая дисциплина, разработанная для проактивного предотвращения перегрузок. Работает путем случайного отбрасывания пакетов до того, как очередь полностью заполнится, сигнализируя TCP-соединениям о необходимости снизить скорость передачи.

Типы очередей **Fair**, **FIFO** и **PRIO**, как правило, не нуждаются в сложной конфигурации.

Настройка параметров RED требует понимания принципов работы алгоритма и влияния каждого параметра на производительность сети. Рекомендуется использовать консервативные значения параметров и тщательно тестировать изменения перед их внедрением в производственной среде.

СВОЙСТВА

band **значения:** 1, 2, 3	Прикрепить очередь к указанной полосе очереди типа prio **условия:** queue = htb && type = class root = true
htb-rate **пример:** 4096, 512k, 10m	Максимальная гарантированная полоса пропускания для этого класса и всех потомков **условия:** queue = htb
htb-ceil **пример:** 4096, 512k, 10m	Полоса пропускания доступная с учётом заимствования **условия:** queue = htb

htb-burst **пример:** 4096, 512k, 10m	Количество байт отправленных на htb-ceil скорости, до переключения на следующий класс **условия:** queue = htb
htb-prio **значения:** 1, 2, 3, 4, 5, 6, 7, 8	Приоритет класса, класс с меньшим приоритетом проверяется раньше **условия:** queue = htb && type = class
htb-default **значения:** /network qos queue	Отправлять весь неклассифицированный трафик в этот класс **условия:** queue = htb && type = qdisc
htb-r2q **минимум:** 1	Частота вычисления DRR квантов для HTB планировщика **условия:** queue = htb && type = qdisc
htb-quantum **минимум:** 1	Сколько байт может передать поток внутри класса **условия:** queue = htb
red-min **минимум:** 1	Средний размер очереди (байт), при котором становится возможной маркировка пакетов **условия:** queue = red
red-max **минимум:** 1	Средний размер очереди (байт), при котором вероятность маркирования достигает максимума **условия:** queue = red
red-probability **пример:** 0, 0.01, 1	Максимальная вероятность маркировки **условия:** queue = red
red-limit **минимум:** 1	Фактический предел очереди (байт). Последующие пакеты будут отброшены **условия:** queue = red
red-burst **минимум:** 1	Интервал (байт) между подгонкой среднего размера очереди к реальному **условия:** queue = red
red-avpkt **минимум:** 1	Размер пакета (байт), используемый для расчёта среднего размера очереди **условия:** queue = red
red-bandwidth **минимум:** 1 **пример:** 4096, 512k, 10m	Скорость интерфейса, используется для расчётов, не ограничивает трафик **условия:** queue = red
red-ecn **значения:** true, false	Explicit Congestion Notification, уведомляет удалённые хосты о превышении полосы пропускания **условия:** queue = red
red-harddrop **значения:** true, false	Принудительно отбрасывасывать пакеты если средний размер очереди превысит значение red-max **условия:** queue = red
red-adaptive **значения:** true, false	Динамически изменять red-probability что бы соответствовать усреднённому размеру очереди **условия:** queue = red

8. peripheral

8.1. gpio

Раздел GPIO предназначен для настройки входов/выходов общего назначения (GPIO) роутера,если они у него есть. Количество доступных для настройки GPIO зависит от возможностей устройства. Физические характеристики и число портов GPIO для конкретного роутера можно узнать в руководстве пользователя и на сайте производителя.

Подавать напряжение на вход GPIO можно только после включения роутера. Несоблюдение данного требования ведёт к выходу роутера из строя и лишению владельца права на гарантийное обслуживание.

На вход GPIO нельзя подавать напряжение превышающее напряжение питания роутера.

В случае если к GPIO не подключен резистор 10 кОм, нельзя допускать разности между напряжением питания роутера и напряжением, подаваемым на вход GPIO. Если резистор 10 кОм установлен, такая разность напряжений допускается.

СВОЙСТВА

direction **значения:** in, out	Направление работы порта **условия:** .type = gpi .type = gpo
value **значения:** high, low	Логический уровень напряжения на порту **условия:** direction = in
trigger **значения:** none, rising, falling, both	Генерировать событие по спаду, по фронту **условия:** direction = in
debounce	Интервал отскока (мсек), нейтрализация дребезга **условия:** direction = in

8.2. poe

Данный раздел предоставляет средства управления и мониторинга для функционала Power over Ethernet (PoE), **доступного только на определенных моделях роутеров, оснащенных соответствующим аппаратным обеспечением**, например на роутерах серии R10.

Роутер оснащен системой «Защитник PoE», которая не только подает питание на подключенные устройства, но и активно отслеживает каждый порт на предмет электрических неисправностей (таких как короткое замыкание или перегрузка по току), а также пытается автоматически восстановить его работу.

Состояние портов и работа

Вы можете отслеживать состояние каждого PoE-порта в реальном времени:

- **Disabled:** Порт административно выключен, питание не подается.
- **Enabled:** Порт активен и успешно подает питание на подключенное устройство.
- **Error:** Обнаружена неисправность, и система автоматически прекратила подачу питания на порт в целях безопасности.

Обработка ошибок и самовосстановление

Когда срабатывает механизм защиты, «Защитник PoE» запускает последовательность автоматического восстановления:

1. Первая попытка восстановления выполняется через **2 секунды** после обнаружения неисправности.
2. Если первая попытка неудачна, вторая попытка выполняется через **5 секунд**.

Если обе попытки неудачны, порт остается в состоянии *Error* для предотвращения повреждения роутера или подключенного устройства и требует ручного вмешательства.

Ручное вмешательство

Для управления портом в состоянии «Error» или для его настройки:

- **Чтобы проверить ошибку:** Выберите конкретный порт, и просмотрите описание последней зафиксированной ошибки и время ее возникновения.
- **Чтобы вручную подать питание:** После устранения физической проблемы с помощью **Apply** повторно перезапустите порт.
- **Чтобы включить/отключить порт:** Выберите нужный порт и измените состояние флажка **Disabled**.

СВОЙСТВА

disabled **значения:** true, false	Не включать PoE на порту при загрузке системы

8.3. protect

Данный раздел предназначен для управления сервисом **protectd**, который обеспечивает активную электрическую защиту для портов ввода-выода общего назначения (GPIO).

Сервис отслеживает GPIO на предмет неисправностей, таких как короткое замыкание или перегрузка по току. При обнаружении сбоя **Protectd** автоматически отключает соответствующий порт, чтобы предотвратить повреждение внутренних цепей роутера. Порт будет оставаться в отключенном состоянии (состоянии ошибки) до тех пор, пока проблема не будет устранена и сервис не будет перезапущен вручную с этой страницы.

Действие перезапуска следует выполнять только после того, как внешняя физическая неисправность (например, короткое замыкание в подключенной проводке) была устранена.

КОМАНДЫ

restart	Перезапуск защиты GPIO

8.4. serial port

Данный раздел предназначен для настройки физических портов RS232 и RS485 роутера, превращая его в многофункциональный шлюз Serial-to-IP. Этот функционал позволяет инкапсулировать данные из последовательного порта в IP-пакеты и передавать их по сети, обеспечивая удаленный доступ и интеграцию традиционного последовательного оборудования в современные IP-системы.

Ключевым элементом конфигурации является **Режим работы**, который определяет, как роутер будет обрабатывать последовательные данные:

- **Server Mode (Режим Сервер):** Роутер ожидает входящие TCP-соединения на указанном порту. Удаленный клиент подключается к роутеру для получения доступа к подключенному последовательному устройству.
- **Client Mode (Режим Клиент):** Роутер активно инициирует исходящее TCP-соединение с удаленным сервером, пересылая на него все данные, полученные с локального последовательного порта.
- **Modbus TCP Mode (Режим Modbus TCP):** Роутер функционирует как шлюз Modbus, преобразуя запросы Modbus TCP из сети в запросы Modbus RTU/ASCII для подключенного ведомого (slave) устройства.
- **NTRIP Client Mode (Режим NTRIP-клиент):** Специализированный режим для подключения к NTRIP Caster с целью получения поправок для систем GNSS и их передачи на подключенное последовательное устройство (например, на высокоточный GPS-приемник).

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
mode **значения:** client, server, modbustcp	Режим работы последовательного порта **условия:** /defaults/ntripclient_installed = true
host	Адрес удалённого хоста **условия:** mode = client
ntrip-mode **значения:** auto, ntrip1, http, rtsp, udp	Транспорт для обмена данными **условия:** mode = ntripclient && ntripclient_installed = true
local-baudrate **значения:** 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	Скорость передачи через последовательный порт
local-parity **значения:** none, odd, even	Контрольный бит чётности
local-stop-bits **значения:** 1, 2	Число стоп-бит в посылке
local-data-bits **значения:** 8, 7	Число бит данных в посылке **условия:** mode = client mode = server mode = ntripclient
local-flowcontrol **значения:** none, soft, hard	Управление потоком
remote-proto **значения:** raw, rfc2217	Протокол последовательно порта удалённой стороны **условия:** mode = client mode = server
remote-baudrate **значения:** 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	Скорость передачи через последовательный порт **условия:** remote-proto = rfc2217 && mode = client

remote-parity **значения:** none, odd, even	Контрольный бит чётности **условия:** remote-proto = rfc2217 && mode = client
remote-stop-bits **значения:** 1, 2	Число стоп-бит в посылке **условия:** remote-proto = rfc2217 && mode = client
remote-data-bits **значения:** 8, 7	Число бит данных в посылке **условия:** remote-proto = rfc2217 && mode = client
remote-flowcontrol **значения:** none, soft, hard	Управление потоком **условия:** remote-proto = rfc2217 && mode = client
remote-acknowledgement **значения:** true, false	Требовать от удалённой стороны подтверждения настроек **условия:** remote-proto = rfc2217 && mode = client
remote-acknowledgement-timeout	Таймаут подтверждения настроек удалённой стороной **условия:** remote-proto = rfc2217 && mode = client
banner	Баннер отправляемый при соединении **условия:** remote-proto = raw && mode = client remote-proto = raw && mode = server
local-accumulation-interval **минимум:** 1	Период (мсек) между чтением данных из последовательного порта в буфер для последующей отправки буфера целиком **условия:** mode != modbustcp
local-accumulation-attempts	Сколько раз читать данные из последовательного порта для накопления буфера **условия:** mode != modbustcp
reconnect-delay **минимум:** 1	Задержка (сек) после разрыва до повторного подключения
peer-timeout **минимум:** 0	Разорвать соединение если удалённая сторона бездействует дольше указанного времени (сек)
bind **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tp-v3, /tunnel atunnel, /defaults server **пример:** bridge0	Выбор интерфейса или адреса для ожидания подключения **условия:** mode = modbustcp mode = server
port **пример:** 80, !80	Порт для ожидания подключения **условия:** mode = modbustcp mode = server
ntrip-mountpoint	Mountpoint или другой критерий согласования набора данных **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-user	Имя пользователя для аутентификации и/или согласования набора данных **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-password	Пароль пользователя **условия:** mode = ntripclient && ntripclient_installed = true

ntrip-nmea	Строка NMEA данных для отправки на сервер **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-bitrate **значения:** true, false	Исходящий bitrate **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-initudp **значения:** true, false	Отправка предварительного UDP пакета для обработки файрволом **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-udpport **пример:** 80, !80	Выбрать локальный UDP порт **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-proxyhost **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес прокси сервера **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-protocol **значения:** none, rts_cts, xon_xoff	Протокол контроля потока для последовательного порта **условия:** mode = ntripclient && ntripclient_installed = true
failopen-timeout	Задержка до коммуникации с последовательным портом после ошибки
debug **значения:** true, false	Режим подробного логгирования

9. service

9.1. client

Раздел предназначен для создания списка клиентов и управления учетными данными пользователей для различных VPN и туннельных сервисов, работающих на роутере (например, L2TP, OpenVPN, PPTP).

Вместо того чтобы определять пользователей в конфигурации каждой отдельной службы, эта страница позволяет создать единый профиль пользователя, который может быть связан с определенным сервисом. Это упрощает управление пользователями и обеспечивает согласованность настроек на всей платформе.

Каждый профиль клиента определяется уникальным именем пользователя (*Name*) и паролем для аутентификации. Также можно назначать атрибуты для каждого клиента, такие как определенный статический *IP-адрес туннеля* и пользовательские *Маршруты*, которые будут переданы клиенту при подключении. Это обеспечивает точный контроль доступа, позволяя определять, к каким именно сетевым ресурсам сможет получить доступ каждый удаленный пользователь.

СВОЙСТВА

disabled **значения:** true, false	Не использовать профиль пользователя
service **значения:** /defaults services	Сервисы, которыми пользователь может пользоваться
password	Пароль пользователя
tunnel-ip **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	IP адрес назначаемый для туннельного интерфейса удалённой стороны

route	Адреса за удалённой стороной для добавления локального маршрута

9.2. dhcp

9.2.1. lease

Подраздел отображает в реальном времени информацию обо всех IP-адресах, выданных встроенным DHCP-сервером роутера. Он служит центральной точкой для мониторинга подключенных к сети устройств и управления назначениями их IP-адресов.

В таблице перечислены все активные аренды с указанием MAC-адреса клиента, назначенного ему IP-адреса и времени истечения аренды.

Основная функция этой страницы — управление арендами, в частности, создание **статических аренд** (также известных как резервирования). Статическая аренда гарантирует, что определенное устройство, идентифицируемое по его MAC-адресу, всегда будет получать один и тот же IP-адрес от DHCP-сервера. Это необходимо для серверов, принтеров и любых других устройств, которым требуется постоянный и предсказуемый сетевой адрес.

Чтобы создать резервирование, вы можете просто выбрать существующую динамическую запись из списка и использовать функцию **Make Static**. Это действие преобразует временное назначение в постоянное. Кроме того, для каждой записи можно настроить интеграцию с DNS, присвоив ей полное доменное имя (FQDN).

КОМАНДЫ

make-static	Сделать динамическую запись lease постоянной

СВОЙСТВА

interface **значения:** /service dhcp server, auto	Интерфейс, на котором может быть выдана статическая запись lease
ip **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	IP адрес хоста
mac **пример:** FE:FF:FF:FF:FF:FF	MAC адрес хоста
dns **значения:** true, false	Добавить DNS запись для разрешения IP адреса
fqdn **пример:** localhost, example.com, sample.example.com	Указать имя хоста для разрешения IP адреса

9.2.2. server

Подраздел предназначен для определения и управления отдельными конфигурациями DHCP-сервера для каждого из ваших локальных сетевых интерфейсов. Это основная панель для настройки способа распределения IP-адресов в заданном сетевом сегменте.

Ключевым выбором на этой странице является Режим работы (**Mode**), который определяет, будет ли роутер выступать в роли DHCP-сервера или в роли агента ретрансляции DHCP.

Режим «Сервер» (Server)

При выборе режима **Server** роутер становится сервером, ответственным за выдачу IP-адресов в определенной сети. Здесь настраиваются основные параметры службы, такие как Диапазон IP-адресов (*Pool Of IP Addresses*) для аренды, Время аренды (*Leasetime*) и важную сетевую информацию, передаваемую клиентам, включая шлюз по умолчанию (*Router*) и DNS-серверы. Этот режим также позволяет выполнять расширенную настройку через пользовательские *DHCP-опции* для поддержки специализированных клиентов и сетевых сред.

Режим «Ретранслятор» (Relay)

При выборе режима **Relay** роутер не выдает IP-адреса самостоятельно. Вместо этого он прослушивает DHCP-запросы на локальном интерфейсе и пересылает их на централизованный удаленный DHCP-сервер. Этот режим обычно используется в корпоративных сетях для управления IP-адресами из единого центра. Настройка в этом режиме включает указание адреса удаленного Сервера и управление обработкой DHCP-опций (в частности, опции 82) при их ретрансляции.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
mode **значения:** server, relay	Режим обработки DHCP запросов
server **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес DHCP сервера для переадресации запросов **условия:** mode = relay
relay-mode **значения:** append, replace, forward, discard	Действие над DHCP пакетом содержащим опцию 82 **условия:** mode = relay && suboption = true mode = relay && suboption = ""
remote-id	Option 82 Remote ID **условия:** mode = relay
hops **максимум:** 255	Максимальное количество прыжков (hop) прежде чем DHCP пакет будет отброшен **условия:** mode = relay
suboption **значения:** true, false	Send link selection suboption for directly connected clients **условия:** mode = relay
debug **значения:** true, false	Режим подробного логгирования **условия:** mode = relay
pool	Пул IP адресов для выдачи клиентам **условия:** mode = server
router **пример:** 192.168.1.1	IP адрес шлюза (Опция 3) **условия:** mode = server
dns-server	IP адрес DNS сервера (Опция 6) **условия:** mode = server
ntp-server	IP адрес NTP сервера (Опция 42) **условия:** mode = server

leasetime **значения:** 30m, 1h, 4h, 12h, 24h, 7d	Время аренды IP адреса **условия:** mode = server
flags **значения:** authoritative, no-override, sequential-ip, rapid-commit	Параметр DHCP сервера **условия:** mode = server
option **значения:** tftp-server, bootfile-name, classless-static-route	Дополнительные DHCP опции **условия:** mode = server

9.3. dns

В этом разделе настраивается DNS-сервер роутера. Он служит общей точкой для обработки DNS-запросов от всех устройств в сети. Роутер пересылает эти запросы на внешние DNS-серверы и запоминает (кэширует) ответы, чтобы ускорить доступ при последующих обращениях к тем же сайтам.

Эта страница предоставляет комплексный контроль над процессом разрешения доменных имен:

- **Логика переадресации DNS:** Вы можете определить основной вышестоящий *DNS-сервер* (или серверы) для всех стандартных запросов. Кроме того, функция **DNS Forwarding** позволяет настроить условную пересылку, направляя запросы для определенных доменов (например, корпоративного домена) на другой набор DNS-серверов.
- **Разрешение локальных имен:** Функция *Static-Host* позволяет создавать собственные локальные DNS-записи, присваивая легко запоминаемые имена хостов устройствам в вашей сети (например, сопоставляя *nas.lan* с *192.168.1.10*).
- **Защита от DNS-rebinding:** Это функция безопасности, которая защищает вашу локальную сеть от соответствующих атак. Она работает, отбрасывая ответы от вышестоящих DNS-серверов, которые указывают на приватные, немаршрутизируемые IP-адреса (RFC1918). Исключения для доверенных сервисов можно настроить для определенных доменов или для DNS-черных списков, использующих localhost.
- **Привязка к интерфейсам:** Вы можете указать, на каких локальных интерфейсах DNS-сервер должен прослушивать запросы от клиентов.

СВОЙСТВА

dns-address	Адрес DNS сервера для пересылки запросов
dns-forwarding	Доменная зона и её DNS сервер для разрешения IP адресов
interface **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server	Интерфейс для обслуживания DNS запросов
static-host	Статическая A-запись DNS
rebind-protection **значения:** true, false	Защита от атаки DNS rebind (отбрасывание ответов с адресом из RFC1918)
rebind-localhost **значения:** true, false	Разрешить ответы с адресом из диапазона 127.0.0.0/8 (DNS based blacklist) **условия:** rebind-protection = true

rebind-domain	Разрешить ответы с адресом из RFC1918 для доменного имени **условия:** rebind-protection = true

9.4. l2tp server

Данный раздел предназначен для настройки встроенного L2TPv2-сервера роутера, это позволяет удаленным пользователям устанавливать безопасные туннели в локальную сеть. Базовая настройка включает в себя определение собственного IP-адреса сервера внутри туннеля и Пула IP-адресов, из которого будут назначаться адреса подключающимся клиентам.

Важнейший выбор конфигурации — это метод шифрования (**Encryption**), который определяет уровень безопасности туннеля:

- **IPsec (Рекомендуется):** Для максимальной безопасности следует использовать L2TP поверх IPsec (*l2tp/ipsec*). При выборе этой опции роутер упрощает конфигурацию, автоматически создавая необходимые IPsec-соединение и правила межсетевого экрана.

После выбора шифрования *ipsec* и применения настроек, вы должны перейти в раздел *Service / IPsec*, чтобы установить **Общий ключ (Pre-Shared Key)** или настроить другой метод аутентификации IPsec для автоматически созданного соединения. Туннель не будет полностью функционировать, пока этот шаг не будет выполнен.

- **MPPE (Microsoft Point-to-Point Encryption):** Это более простой, интегрированный метод шифрования, который автоматически используется в паре с аутентификацией MS-CHAPv2. Он подходит для клиентов, которые не поддерживают IPsec.
- **Без шифрования (None):** Нешифрованный туннель L2TP. Этот вариант категорически не рекомендуется для использования в публичных сетях.

L2TP-сервер будет аутентифицировать клиентов по профилям пользователей, настроенным в разделе *Service / Clients*.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
ip-addr **пример:** 192.168.1.1	IP адрес туннельного интерфейса
ip-pool	Диапазон IP адресов, назначаемых клиентам
auth **значения:** any, chap, mschap, mschap-v2, pap, eap	Выбор протокола для аутентификации **условия:** encryption = mppe
encryption **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point

debug **значения:** true, false	Режим подробного логгирования

9.5. ntp

Раздел NTP предназначен для настройки текущего времени на устройстве.

Этот раздел настраивает сервис протокола сетевого времени (Network Time Protocol, NTP), который отвечает за поддержание точного системного времени на роутере. Точное время является обязательным требованием для корректного ведения журналов, действительной аутентификации по сертификатам и правильного функционирования многих сетевых протоколов.

Роутер может работать в двух различных ролях:

- **NTP-клиент (Синхронизация времени)** - В своей основной роли NTP-клиента роутер синхронизирует собственные часы с внешними, авторитетными серверами времени. Вы указываете эти вышестоящие серверы в списке *Pool*. Роутер будет периодически опрашивать эти серверы, чтобы обеспечить постоянную точность своих внутренних часов.
- **NTP-сервер (Источник времени для локальной сети)** -
  При включении опции *Server*, роутер сам становится NTP-сервером для вашей локальной сети. Клиентские устройства в локальной сети могут быть настроены на использование IP-адреса роутера в качестве источника времени. Это обеспечивает идеальную синхронизацию всех устройств в вашей локальной сети и сокращает объем NTP-трафика, направляемого в интернет.

Мониторинг статуса синхронизации

Функция **Info** предоставляет доступ к подробной таблице состояния соединений роутера с его вышестоящими NTP-серверами.

КОМАНДЫ

info	Информация о состоянии NTP клиента

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
pool	Пул серверов для синхронизации
server **значения:** true, false	Разрешить обрабатывать NTP запросы клиентов

9.6. openvpn server

Данный раздел позволяет настроить роутер в качестве надежного и гибко настраиваемого сервера OpenVPN.

Инфраструктура открытых ключей (PKI) и ключи

Безопасная работа основана на наборе сертификатов и ключей:

- **CA Certificate:** Файл *Ca* является корнем доверия для вашего VPN. Все клиентские и серверные сертификаты должны быть подписаны этим Центром Сертификации.

- **Сертификат сервера:** *Cert* — это публичный сертификат сервера, который он предъявляет клиентам для подтверждения своей подлинности.
- **Ключ TLS-аутентификации:** Ключ *Tls-Auth* обеспечивает дополнительный уровень HMAC-аутентификации для канала управления, повышая устойчивость сервера к DoS-атакам и сканированию портов. Вы можете создать новый ключ с помощью функции **Generate TA Key**. Этот ключ сохраняется в разделе *Storage* / *File* и должен быть передан всем клиентам.

Аутентификация пользователей

OpenVPN поддерживает два основных метода аутентификации клиентов:

1. **Аутентификация только по сертификату:** Доступ предоставляется исключительно на основании валидного клиентского сертификата, подписанного CA сервера. Имя пользователя и пароль не требуются.
2. **Аутентификация по сертификату и имени пользователя/паролю:** Обеспечивает двухфакторную аутентификацию. Доступ предоставляется, только если **одновременно** предъявлен валидный клиентский сертификат и введены верные имя пользователя и пароль. Логика проверки следующая:
    - Если имя пользователя не существует на роутере, доступ **запрещен**.
    - Если имя пользователя существует, но пароль не совпадает, доступ **запрещен**.
    - Если имя пользователя и пароль верны, доступ **разрешен**.

Для включения аутентификации по имени пользователя и паролю, нужно создать соответствующий профиль для этого пользователя в разделе *Service* / *Clients*, обязательно указав для него пароль.

КОМАНДЫ

generate-ta-key	Сгенерировать файл случайного ключа, используемый как TA Key или Static Key filename - Имя конфигурации (обязательно)

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
dev-type **значения:** tun, tap	Тип виртуального интерфейса
protocol **значения:** tcp, udp	Транспортный протокол туннеля
port **пример:** 80, !80	Порт для входящих подключений
tunnel-ip **пример:** 192.168.1.1/24	Адрес туннельного интерфейса
pool **пример:** 192.168.1.100, 192.168.1.1-192.168.1.100	Пул IP адресов для выдачи клиентам
cipher **значения:** AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-192-GCM, AES-256-CBC, AES-256-GCM	Алгоритм шифрования туннеля

auth **значения:** MD5, SHA1, SHA256, SHA384, SHA512	HMAC алгоритм для аутентификации
ta-key **значения:** /storage file	Ключ дополнительной HMAC аутентификации
ca **значения:** /storage certificate	Публичный ключ удостоверяющего цетра (CA)
cert **значения:** /storage certificate	Локальный сертификат (включая приватный ключ)
keepalive **пример:** 10 60	Настроить ping клиентского соединения и перезапуск в случае недоступности
push **значения:** route, route-gateway, route-metric, route-delay, redirect-gateway, ip-win32, dhcp-option, inactive, ping, ping-exit, ping-restart, setenv, auth-token, persist-key, persist-tun, topology, echo, comp-lzo, socket-flags, sndbuf, rcvbuf	Отправить выбранные параметры в клиентскую конфигурацию
flag **значения:** allow-recursive-routing, auth-nocache, client-to-client, comp-noadapt, disable, duplicate-cn, fast-io, float, mtu-test, multihome, ncp-disable, nobind, opt-verify, passtos, persist-key, persist-local-ip, persist-remote-ip, persist-tun, ping-timer-rem, pull, push-peer-info, push-reset, remote-random, route-nopull, single-session, suppress-timestamps, tcp-nodelay, tls-client, tls-exit, tls-server, username-as-common-name	Дополнительные опции туннеля
extra **значения:** auth-retry, bcast-buffers, comp-lzo, compress, connect-freq, connect-retry, connect-retry-max, connect-timeout, ecdh-curve, explicit-exit-notify, fragment, hand-window, hash-size, ifconfig-pool-netmask, ifconfig-push-local, ifconfig-push-netmask, inactive, key-direction, keysize, link-mtu, max-clients, mssfix, mtu-disc, ping, ping-exit, ping-restart, prng, pull-filter-accept, pull-filter-ignore, pull-filter-reject, rcvbuf, reneg-bytes, reneg-pkts, reneg-sec, replay-persist, replay-window, resolv-retry, shaper, sndbuf, tcp-queue-limit, tls-timeout, tls-version-min, tran-window, tun-mtu, tun-mtu-extra, txqueuelen, verb, verify-client-cert, verify-x509-name, x509-username-field	Дополнительные параметры туннеля

9.7. pinger

Раздел Pinger настраивает автоматическую службу, выполняющую две основные задачи: общий мониторинг соединений и динамическое управление отказоустойчивостью WAN-каналов.

В качестве инструмента мониторинга он может быть настроен на периодическую проверку доступности любого целевого хоста с помощью различных типов проверок (ICMP, TCP и т.д.). Это позволяет отслеживать состояние любого важного канала или сервиса.

Однако его основное автоматическое действие — это управление приоритетом маршрутизации для обеспечения отказоустойчивости.

Когда Pinger обнаруживает ухудшение качества такого маршрута — на основе заданных пользователем порогов — он автоматически **увеличивает метрику** этого маршрута.

Автоматическое изменение метрики применяется **специально и исключительно к тем интерфейсам, которые настроены как «Маршрут по умолчанию»**.

Это действие понижает приоритет проблемного канала, в результате чего система маршрутизации автоматически отдает предпочтение альтернативному маршруту по умолчанию с лучшей (более низкой) метрикой.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
type **значения:** icmp, arping, http, tcp	Метод проверки доступности сетевого узла
host	Список адресов для проверки доступности сетевого узла **условия:** type = tcp
interval **минимум:** 10	Интервал между проверками
retries **минимум:** 1	Порог неудачных проверок до перезапуска интерфейса
count **минимум:** 1	Число пакетов для проверки в рамках одной попытки **условия:** type = arping type = http type = icmp
size **минимум:** 1, **максимум:** 65535	Размер пакета **условия:** type != http
rtt-threshold	Порог round-trip времени, превышение которого считается неудачей
loss-threshold	Порог потерянных пакетов, превышение которого считается неудачей **условия:** type = icmp type = arping

9.8. pptp server

Данный раздел настраивает встроенный сервер PPTP (Point-to-Point Tunneling Protocol). Он позволяет удаленным пользователям устанавливать VPN-туннель для доступа в локальную сеть.

Базовая настройка включает определение собственного IP-адреса сервера внутри туннеля и пула IP-адресов, из которого будут назначаться адреса подключающимся клиентам.

Важнейший выбор конфигурации — это метод **Шифрования**, который определяет уровень безопасности туннеля:

- **IPsec (Рекомендуется для безопасности):** Эта опция инкапсулирует трафик PPTP в защищенный IPsec-туннель. Для упрощения этой сложной настройки роутер **автоматически сгенерирует** необходимую конфигурацию при включении этого режима:
- IPsec-соединение (*pptp_server_connection*) и ассоциацию (*pptp_server_association*) в разделе *Service / IPsec*.
- Соответствующее правило межсетевого экрана в *Firewall / Filter* (*pptp_server_autogenerated*).

Для корректной работы IPsec-туннеля требуется выполнить действие вручную. После применения настроек вы **должны** перейти в раздел *Service / IPsec / Connection*, выбрать запись *pptp_server_connection* и настроить метод аутентификации (например, указать Общий ключ / Pre-Shared Key). Соединение не будет работать, пока этот шаг не будет выполнен.

- **MPPE (Microsoft Point-to-Point Encryption):** Предоставляет более простой, интегрированный метод шифрования, который автоматически работает в паре с протоколом аутентификации MS-CHAPv2.
- **None (Без шифрования):** Нешифрованный туннель PPTP. Этот вариант **категорически не рекомендуется** для использования в публичных сетях, так как он не обеспечивает конфиденциальность данных.

Аутентификация пользователей управляется централизованно в разделе *Service / Clients*.

При указании диапазона для полей **IP Addresses** и **IP Pool** необходимо учитывать его последующее преобразование в определенный синтаксис. Примеры:

• 1.1.1.2-1.1.1.10 → 1.1.1.2-10

• 1.1.2.3-1.1.5.10 → 1.1.2-5.10 (т.е. от 1.1.2.10 до 1.1.5.10)

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
ip-addr	IP адрес туннельного интерфейса
ip-pool	Диапазон IP адресов, назначаемых клиентам
auth **значения:** any, chap, mschap, mschap-v2, pap, eap	Выбор протокола для аутентификации **условия:** encryption = mppe
encryption **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point
debug **значения:** true, false	Режим подробного логгирования

9.9. snmp

Данный раздел настраивает встроенный SNMP-агент (Simple Network Management Protocol) роутера, который позволяет устройству взаимодействовать с централизованной Системой Управления Сетью (NMS). Протокол SNMP предоставляет стандартизированный доступ к широкому спектру операционных данных, таких как загрузка ЦП, использование памяти, статистика интерфейсов и уровень сигнала сотовой связи.

Роутер поддерживает две основные версии протокола, каждая из которых предлагает свой уровень безопасности.

SNMPv2c

Это более простая и широко используемая версия, которая использует для контроля доступа *Community-строку*. Эта строка действует как общий пароль между роутером и системой

управления.

Community-строка передается по сети в открытом виде. Поэтому протокол SNMPv2c следует использовать только в доверенных, защищенных сетях.

SNMPv3

Эта версия предоставляет надежную и современную модель безопасности, основанную на аутентификации пользователя и шифровании данных (USM - User-based Security Model). Уровень безопасности гибко настраивается.

Разрешение на запись

Опция *Writable*, доступная для обеих версий, позволяет системе управления не только считывать данные (GET-запросы), но и отправлять команды для изменения состояния роутера (SET-запросы), например, для управления GPIO. Эту опцию следует включать с особой осторожностью и только при необходимости.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
version **значения:** v2c, v3	Версия протокола
port **пример:** 80, !80	Порт для обслуживания входящих запросов
community **пример:** bridge0, vpn-client1, user_1@example.com	Community, критерий для аутентификации входящих запросов
sys-name **пример:** bridge0, vpn, client_1	Имя устройства для идентификации в системе мониторинга
sys-contact	Контактные данные устройства для идентификации в системе мониторинга
sys-location	Локация устройства для идентификации в системе мониторинга
sys-description	Описание устройства для идентификации в системе мониторинга
username	Имя пользователя **условия:** version = v3
auth-passphrase **мин. длина:** 8	Парольная фраза (SHA) для аутентификации **условия:** version = v3
priv-passphrase **мин. длина:** 8	Парольная фраза (SHA) для шифрования трафика **условия:** version = v3
security-level **значения:** noauth, auth, priv	Уровень защиты данных при опросе **условия:** version = v3
writable **значения:** true, false	Разрешить вносить изменения и управлять роутером

9.10. vrrp

Данный раздел предназначен для настройки протокола VRRP (Virtual Router Redundancy Protocol) — стандартного протокола, разработанного для обеспечения высокой доступности шлюза по

умолчанию. Он достигает этого путем объединения двух или более роутеров в единый «виртуальный маршрутизатор», который предоставляет всем клиентам в сети один постоянный виртуальный IP-адрес.

Внутри этой группы один роутер избирается как **Master (основной)**, активно обрабатывая трафик, в то время как остальные выступают в роли **Backup (резервных)**. Выбор определяется значением приоритета (чем выше значение в поле *Priority*, тем выше приоритет). В случае сбоя Master-роутера, его роль автоматически перехватывает резервный с самым высоким приоритетом.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
virtual-ip	Виртуальный IP адрес выступающий шлюзом по умолчанию для сети
virtual-mac **значения:** true, false	Назначить виртуальный MAC адрес интерфейсу
preemption-mode **значения:** true, false	Разрешить перехват роли master если приоритет маршрутизатора выше
virtual-id **минимум:** 1, **максимум:** 255	Идентификатор виртуального маршрутизатора
priority **минимум:** 1, **максимум:** 255	Приоритет VRRP маршрутизатора
delay **минимум:** 1, **максимум:** 3600	Интервал (сек) между отправкой VRRP-advertise сообщений
auth **значения:** none, pw, ah	Тип аутентификации для протокола
key **мин. длина:** 1, **макс. длина:** 8	Парольная фраза для аутентификации пакетов VRRP **условия:** auth = ah auth = pw

9.11. zabbix

Данный раздел предназначен для настройки встроенного Zabbix-агента, который позволяет осуществлять мониторинг состояния и производительности роутера с помощью Zabbix-сервера. Агент может работать в двух режимах, которые могут использоваться одновременно.

Режимы работы

- **Пассивные проверки:** В этом режиме Zabbix-сервер сам подключается к агенту на роутере для запроса данных. Необходимо указать IP-адрес *Сервера*, с которого разрешены входящие соединения. Этот режим требует, чтобы порт агента (по умолчанию 10050) был доступен для Zabbix-сервера.
- **Активные проверки:** В этом режиме агент сам инициирует соединение с Zabbix-сервером для отправки данных. Этот режим часто предпочтительнее для устройств, находящихся за межсетевым экраном или NAT. Необходимо указать адрес *Server Active*, чтобы агент знал, куда отправлять данные.

Настройка безопасности (TLS)

Вы можете защитить обмен данными между агентом и сервером с помощью шифрования TLS. Метод шифрования настраивается независимо для пассивных (*TLSAccept*) и активных (*TLSConnect*) режимов:

- **psk:** Шифрование с использованием общего ключа (Pre-Shared Key) и идентификатора.
- **cert:** Шифрование с использованием SSL-сертификатов для аутентификации.
- **unencrypted:** Обмен данными происходит в открытом виде (не рекомендуется для публичных сетей).

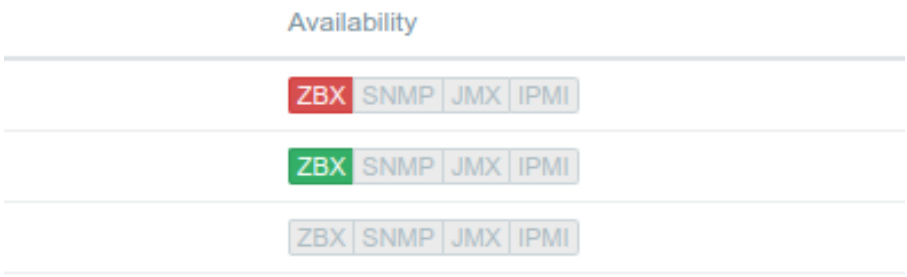
Настройка Zabbix-сервера

Для упрощения интеграции вы можете скачать готовый шаблон для Zabbix-сервера из Базы знаний.

Предоставляемый шаблон предназначен **только для настройки активных проверок** (Zabbix agent active).

Для работы в пассивном режиме необходимо настроить все элементы данных и триггеры на Zabbix-сервере вручную.

Индикатор доступности агента на сервере (значок ZBX в столбце «Доступность») отображает состояние **пассивных проверок**:



- **Горит зеленым:** Пассивные проверки проходят успешно.
- **Горит красным:** Есть проблема с пассивными проверками (например, таймаут, сетевая недоступность).
- **Не подсвечен (серый):** Для узла сети не настроены пассивные проверки (например, если используется шаблон только с активными проверками).

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
hostname	Уникальное имя устройства для идентификации на сервере
port **минимум:** 1024, **максимум:** 32767	Порт для приёма пассивных проверок с сервера
server	Адрес сервера, с которого принимаются входящие подключения
server-active	Адрес сервера для отправки результатов активных проверок
tls-accept **значения:** unencrypted, psk, cert	Тип шифрования для приема входящих подключений

tls-connect **значения:** unencrypted, psk, cert	Тип шифрования для исходящих соединений
ca **значения:** /storage certificate	Публичный ключ удостоверяющего цетра (CA) **условия:** tls-connect = cert tls-accept = cert
cert **значения:** /storage certificate	Сертификат для аутентификации и шифрования **условия:** tls-connect = cert tls-accept = cert
psk **мин. длина:** 32, **макс. длина:** 128 **пример:** 001d6bbe06dc9ad18824a4a78b699805, e560cb0d918d26d31b4f642181f5f570ad89a390931102e539	Pre-shared Key для шифрования подключений **условия:** tls-connect = psk tls-accept = psk
identity	PSK identity string **условия:** tls-connect = psk tls-accept = psk

10. storage

10.1. certificate

Данный раздел предназначен для управления учетными данными TLS (сертификатами и закрытыми ключами). Эти данные необходимы для обеспечения безопасности сервисов, работающих на роутере, таких как веб-интерфейс (HTTPS), OpenVPN, IPsec и других.

Создание и получение учетных данных

Вы можете получить сертификаты для роутера несколькими способами:

- **Create CSR (Запрос на подпись сертификата):** Это стандартный метод для получения сертификата от доверенного публичного Центра Сертификации (ЦС). Вы создаете CSR, отправляете его в ЦС, и взамен получаете подписанный сертификат, который затем можно импортировать.
- **Create X509:** Эта опция генерирует **самоподписанный сертификат**. Он полезен для внутренних сетей, тестирования или в сценариях, где не требуется сертификат, которому доверяют публично.
- **Sign CSR:** Позволяет самому роутеру выступать в роли миниатюрного Центра Сертификации. Вы можете принять CSR от другого устройства (например, другого роутера или клиента) и подписать его с помощью сертификата ЦС, хранящегося на этом роутере.
- **Cert Import:** Используйте эту функцию для загрузки существующих сертификатов и закрытых ключей, которые были созданы на стороне.

Управление и развертывание учетных данных

После того как сертификат попадает в хранилище, им можно управлять:

- **Cert Export:** Позволяет создавать резервные копии учетных данных или распространять их среди клиентов. Экспорт выполняется в стандартном, защищенном паролем формате PKCS12, который может объединить сертификат, его закрытый ключ и все промежуточные сертификаты в один файл.

КОМАНДЫ

cert-create	Создать сертификат name - Имя нового файла (обязательно) ca - Сертификат удостоверяющего цетра (CA) authority - Сертификат может быть использован для подписания pkey-size - Размер приватного ключа cn - Имя субъекта (обязательно) alt-name - Альтернативное имя субъекта org - Имя организации субъекта unit - Юнит организации субъекта state - Область субъекта country - Страна субъекта location - Местоположение субъекта days - Срок действия сертификата
csr-create	Создать CSR файл name - Имя нового файла CSR (обязательно) pkey-size - Размер публичного ключа passphrase - Парольная фраза для файла сертификата cn - Имя субъекта (обязательно) alt-name - Альтернативное имя субъекта org - Имя организации субъекта unit - Юнит организации субъекта state - Область субъекта country - Страна субъекта location - Местоположение субъекта
csr-sign	Подписать CSR name - CSR файл для подписания (обязательно) ca - Сертификат удостоверяющего цетра (CA) (обязательно) alt-name - Альтернативное имя субъекта days - Срок действия подписанного сертификата passphrase - Парольная фраза для файла сертификата
cert-export	Экспорт сертификата в формате PKCS12 name - Файл сертификата для экспорта (обязательно) include-pkey - Вложить приватный ключ в экспортируемый файл passphrase - Парольная фраза для файла сертификата additional-cert - Добавить дополнительный сертификат в связку
cert-import	Импорт сертификата name - Файл сертификата для импорта (обязательно) passphrase - Парольная фраза для файла сертификата
rename	Изменить имя файла сертификата new-name - Имя нового файла (обязательно)

СВОЙСТВА

issuer	Наименование центра сертификации, выдавшего сертификат
subject	Наименование субъекта
alt-name	Альтернативное Наименование субъекта **условия:** alt-name != ""
not-before	Дата, до которой сертификат не действителен
not-after	Дата, после которой сертификат не действителен
fingerprint	Хэш сертификата

10.2. file

Данный раздел представляет собой интерфейс для управления файлами, хранящимися на роутере. Он служит основным инструментом для загрузки, скачивания и организации файлов, необходимых для различных системных операций, таких как резервные копии конфигурации, образы прошивок или пользовательские скрипты.

Файловый менеджер различает два основных места хранения:

- **Временное хранилище:** Файлы здесь находятся в энергозависимой памяти (ОЗУ) и будут утеряны при перезагрузке системы. Это место обычно используется как промежуточная область для файлов перед их установкой или импортом определенным сервисом.
- **Постоянное хранилище:** Файлы здесь записываются в энергонезависимую флеш-память роутера и сохраняются между перезагрузками.

С помощью этого интерфейса можно загружать новые файлы, скачивать существующие, перемещать их между хранилищами или удалять. Кроме того, можно управлять правами доступа к файлам, устанавливая флаг «Исполняемый» (*Executable*) для скриптов.

КОМАНДЫ

upload	Загрузить файл
download	Загрузить файл с устройства
import	Импорт файла на устройство

СВОЙСТВА

file-type	Тип файла
file-size	Размер файла
last-change	Время последнего изменения файла
last-access	Время последнего открытия файла

11. system

11.1. access

11.1.1. radius

В данном разделе выполняется настройка централизованной аутентификации и авторизации пользователей по протоколу **Remote Authentication Dial-In User Service (RADIUS)**.

При использовании данной схемы роутер выступает в роли **сервера сетевого доступа (Network Access Server, NAS)**. При попытке входа в систему устройство передает учетные данные пользователя на выделенный RADIUS-сервер для проверки подлинности. Для взаимодействия требуется уникальный идентификатор роутера и корректный секретный ключ для авторизации на стороне сервера.

СВОЙСТВА

disabled **значения:** true, false	Отключить Radius аутентификацию
server **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Сервер аутентификации
nas-id **макс. длина:** 32 **пример:** bridge0, vpn-client1, user_1@example.com	Уникальный идентификатор NAS
secret	Пароль для аутентификации NAS на RADIUS сервере

11.1.2. ssh

Данный раздел предназначен для настройки встроенного SSH-сервера роутера, который предоставляет безопасный, зашифрованный доступ к командной строке для расширенного администрирования, настройки и диагностики.

Помимо включения или отключения службы и изменения прослушиваемого порта, в разделе можно настроить криптографические алгоритмы, используемыми SSH-сервером. Это позволяет администраторам усилить профиль безопасности устройства, отключая более слабые алгоритмы и обеспечивая соответствие определенным корпоративным или нормативным политикам безопасности.

Можно настроить следующие криптографические компоненты:

- **Cipher:** Определяет алгоритмы симметричного шифрования для обеспечения конфиденциальности данных.
- **Host Key Algorithms:** Определяет алгоритмы открытого ключа, которые сервер может использовать для подтверждения своей подлинности.
- **KEX Algorithms:** Управляет методами, используемыми для безопасной генерации и обмена сеансовыми ключами.
- **MAC Algorithms:** Указывает алгоритмы хеширования, используемые для обеспечения целостности и подлинности сообщений.

Изменение этих криптографических настроек предназначено для опытных пользователей. Некорректная конфигурация может привести к невозможности подключиться к роутеру по SSH. Изменяйте эти параметры только в том случае, если это требуется для соответствия определенной политике безопасности.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
port **пример:** 22, 51820	Порт SSH подключения
cipher **значения:** chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com	Выбор определённого алгоритма шифрования
host-key-alg **значения:** rsa-sha2-512, rsa-sha2-256, ssh-rsa, ssh-ed25519	Выбор определённого алгоритма аутентификации
kex-alg **значения:** curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256	Выбор определённого алгоритма обмена ключами
mac-alg **значения:** umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1	Выбор определённого алгоритма проверки целостности

11.1.3. web

Данный раздел предназначен для настройки доступа к веб-интерфейсу управления роутером. Он позволяет управлять протоколами (HTTP/HTTPS) и портами, используемыми для административного доступа.

Основной настройкой является включение безопасного доступа по **HTTPS** с помощью функции *Use HTTPS*. Это шифрует все взаимодействие между вашим браузером и роутером, защищая ваши учетные данные и данные конфигурации от перехвата. Хотя доступ по стандартному **HTTP** возможен, он не является зашифрованным и должен использоваться только в полностью доверенных сетях.

Для включения HTTPS необходимо выбрать *Файл сертификата* (публичный сертификат сервера) и *Файл ключа* (соответствующий ему закрытый ключ) из хранилища сертификатов. Использование собственного, доверенного сертификата устраняет предупреждения безопасности в браузере и обеспечивает защищенный административный сеанс.

Для дополнительного усиления безопасности вы можете:

- Изменить прослушиваемый *Порт* со значения по умолчанию на нестандартный.
- Указать минимальную версию протокола TLS (*TLS Minimum*), чтобы обеспечить использование современных, безопасных криптографических стандартов.

СВОЙСТВА

use-http **значения:** true, false	Разрешить доступ по HTTP
http-port **пример:** 80, !80	Порт для обработки входящих HTTP запросов **условия:** use-http = true
use-https **значения:** true, false	Разрешить доступ по HTTPS
https-port **пример:** 80, !80	Порт для обработки входящих HTTPS запросов **условия:** use-https = true
cert **значения:** /storage certificate	Сертификат для аутентификации и шифрования **условия:** use-https = true
tls **значения:** 1.1, 1.2, 1.3	Минимальная разрешенная версия TLS **условия:** use-https = true
redirect-to-https **значения:** true, false	Перенаправлять входящие HTTP запросы на HTTPS порт **условия:** use-https = true && use-http = true

11.2. config

Этот раздел предоставляет инструменты для управления конфигурацией роутера. Система использует двухэтапную модель конфигурации: изменения сначала вносятся во временную, «кандидатскую» конфигурацию и должны быть явно зафиксированы (*commit*), прежде чем они станут частью постоянной, «текущей» (running) конфигурации.

Конфигурационный файл содержит в себе основной набор параметров для работы роутера. В частности элементами конфигурации роутера могут быть: пароли, ключи, хэши и сертификаты для работы различных служб.

Импорт конфигурации от несовместимой версии прошивки или другой модели устройства может привести к нестабильной работе или сделать устройство недоступным после фиксации изменений.

КОМАНДЫ

revert	Откатить все изменения
commit	Сохранить текущую запущенную конфигурацию
export	Экспорт текущей запущенной конфигурации
import	Импорт файла конфигурации file - Файл конфигурации для импорта (обязательно)
default	Вернуть настройки по умолчанию

11.3. logging

Данный раздел настраивает работу службы системного журнала, которая регистрирует все значимые операционные события: от входа пользователей и изменения настроек до ошибок и системных предупреждений. Эта страница позволяет вам управлять местом назначения и способом хранения этих важных сообщений.

Ведение журнала может осуществляться в двух основных направлениях:

- **На удаленный Syslog-сервер:** Эта функция позволяет в реальном времени отправлять сообщения журнала на удаленный сервер. Вы можете указать адрес сервера и транспортный протокол (например, UDP или TCP). Опция *Prefix* позволяет легко идентифицировать сообщения от данного устройства на центральном сервере.
- **В локальный файл:** В качестве альтернативы вы можете включить опцию *Log to file*, чтобы хранить журналы локально на роутере. Это полезно для диагностики и устранения неисправностей на самом устройстве, особенно когда удаленный сервер недоступен.

Размер файла журнала, отображаемый в разделе */storage/file*, может иметь нулевое значение, даже если ведение журнала в файл активно. Это связано с тем, что значение не обновляется в реальном времени. Для принудительного обновления и отображения актуального размера необходимо нажать непосредственно на **file** в пути к разделу.

СВОЙСТВА

remote-host **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Удалённая сторона для приёма лога
remote-proto **значения:** tcp, udp	Транспортный протокол для отправки лога
remote-prefix	Префикс для записей, отправляемых на удалённый сервер
file-log **значения:** true, false	Записывать лог в файл
file-name	Имя файла для записи лога **условия:** file-log = true

file-size **минимум:** 1, **максимум:** 8192	Не превышать указанный размер (Кбайт) файла **условия:** file-log = true

11.4. management

Этот раздел является основным местом для настройки базовых системных параметров и выполнения важных операций по обслуживанию.

Он позволяет определить идентификационные параметры роутера (такие как имя хоста и часовой пояс) и выполнять общесистемные команды. Отсюда можно перезагрузить устройство, обновить прошивку, выполнить сброс к заводским настройкам или сгенерировать диагностический отчет для устранения неисправностей.

КОМАНДЫ

change	Изменить локальное время и дату на устройстве isotime - Изменить локальное время на устройстве isodate - Изменить локальную дату устройстве
report	Получить отчёт об ошибках устройства
reboot	Перезагрузить устройство
upgrade	Обновить встроенное ПО file - Файл во временной памяти (обязательно) reset - Вернуть настройки по умолчанию

СВОЙСТВА

hostname **пример:** localhost, example.com, sample.example.com	Hostname устройства
timezone **значения:** UTC-12, UTC-11, UTC-10, UTC-9, UTC-8, UTC-7, UTC-6, UTC-5, UTC-4, UTC-3, UTC-2, UTC-1, UTC, UTC+1, UTC+2, UTC+3, UTC+4, UTC+5, UTC+6, UTC+7, UTC+8, UTC+9, UTC+10, UTC+11, UTC+12, UTC+13, UTC+14	Часовой пояс устройства

11.5. package

Данный раздел предоставляет интерфейс для управления программными пакетами, установленными на роутер. Он позволяет расширять функциональность устройства путем установки новых приложений или библиотек.

На странице отображается список всех установленных пакетов, а также информация о них, такая как *версия*, *зависимости*, *размер* и краткое *описание*.

Управление пакетами

- **Установка пакета:** *Install* позволяет выбрать файл пакета (например, в формате *.ipk*), который был предварительно загружен во временное хранилище роутера.
- **Удаление пакета:** *Clean* используется для удаления (деинсталляции) выбранного пакета из системы.

КОМАНДЫ

install	Установить пакет file - Файл во временной памяти (обязательно)

СВОЙСТВА

version	Версия установленного пакета
depends	Зависимости пакета
size	Количество место занимаемого установленными файлами
description	Описание пакета, предоставленное разработчиком

11.6. user

Данный раздел предназначен для создания, управления и определения прав доступа для всех учетных записей, которые могут входить в интерфейс управления роутером.

Система предоставляет полный контроль как над аутентификацией (как пользователи входят в систему), так и над авторизацией (что они могут делать после входа).

Методы аутентификации

Поддерживаются два основных метода аутентификации:

- **Пароль:** Традиционный вход в систему по паролю. Здесь можно установить или изменить пароль пользователя.
- **Ключ SSH:** Более безопасная, беспарольная аутентификация с использованием криптографии с открытым ключом. Можно импортировать публичный SSH-ключ пользователя, что позволит ему входить в систему по SSH без пароля.

Авторизация и контроль доступа

Права доступа управляются через ролевую модель, которая может быть дополнительно уточнена с помощью конкретных ограничений:

- **Уровень доступа (Level):** Каждому пользователю назначается основная роль:
- *administrator*: Имеет полный, неограниченный доступ ко всем настройкам системы.
- *user*: По умолчанию имеет ограниченный доступ только на чтение, который можно настроить.
- **Запрещенные меню (Denied):** Для более детального контроля можно явно заблокировать пользователю доступ к определенным пунктам меню, добавив их в список *denied*.

Управление учетной записью

Помимо определения прав доступа, можно временно отозвать доступ пользователю без удаления профиля.

КОМАНДЫ

password sha256	Изменить пароль пользователя new - Парольная фраза (Plain text или hash [md5 sha512], как в /etc/shadow)
import-ssh-key	Импорт SSH ключа пользователя file - Файл ключа во временной памяти

СВОЙСТВА

disabled **значения:** true, false	Отключить пользователя, запретить доступ
denied **значения:** /defaults schemas	Элементы меню, не доступные для пользователя
level **значения:** administrator, user	Уровень доступа для пользователя
ssh-keys **значения:** $ssh-keys	Ключ пользователя для SSH подключения **условия:** ssh-keys != ""

12. tools

Этот раздел предоставляет набор утилит для диагностики сети и устранения неполадок, которые запускаются по требованию. В отличие от разделов конфигурации, инструменты здесь выполняют разовые действия для анализа и решения проблем в реальном времени.

Доступные утилиты позволяют выполнять спектр диагностических задач, таких как проверка доступности сети на различных уровнях, анализ сетевого трафика, инициирование клиентских сессий на удаленные хосты, а также прямой просмотр системных журналов или загрузка файлов.

КОМАНДЫ

download	Загрузить файл на устройство url - Адрес ресурса (обязательно) to-file - Сохранить файл с этим именем username - Имя пользователя для аутентификации password - Пароль для аутентификации
ping	Ping удалённого узла host - Адрес хоста (обязательно) interface - Интерфейс count - Число отправляемых пакетов size - Размер пакета
sniffer	Сетевой анализатор пакетов interface - Интерфейс для захвата пакетов (обязательно) proto - Фильтр по протоколу src-addr - Фильтр по IP адресу источника пакета dst-addr - Фильтр по IP адресу назначения пакета src-port - Фильтр по порту источника пакета dst-port - Фильтр по порту назначения пакета src-mac - Фильтр по MAC адресу источника пакета dst-mac - Фильтр по MAC адресу назначения пакета append - Логический оператор связывания для фильтров count - Число отправляемых пакетов file - Сохранить дамп пакетов в файл
arping	ARP Ping удалённого узла host - Адрес хоста (обязательно) interface - Интерфейс (обязательно) count - Число отправляемых пакетов
traceroute	traceroute к удалённому узлу host - Адрес хоста (обязательно) max_hops - Предельное количество прыжков до узла protocol - Использовать ICMP Echo пакеты вместо UDP датаграм port - Порт приложения
telnet	Telnet подключение к удалённому узлу host - Адрес хоста (обязательно) interface - Интерфейс port - Порт приложения

journal	Открыть системный журнал filter - Регулярное выражение для фильтрации вывода last - Показать последние N-строк
dashboard	Сводная информация о системе
ssh	SSH подключение к удалённому узлу host - Адрес хоста (обязательно) username - Имя пользователя (обязательно) port - Порт приложения

13. tunnel

13.1. eoip

Данный раздел предназначен для настройки туннелей Ethernet over IP (EoIP) — протокола для создания прозрачного сетевого моста 2-го уровня между двумя удаленными точками через IP-сеть.

Туннель EoIP инкапсулирует полные Ethernet-кадры в IP-пакеты, фактически создавая виртуальное соединение "точка-точка" между двумя роутерами. Основной сценарий использования — бесшовное объединение двух раздельных сегментов LAN в единый широковещательный домен, в результате чего они ведут себя так, как будто соединены физическим Ethernet-кабелем.

Протокол EoIP, изначально разработанный компанией MikroTik, является простым и эффективным решением для расширения сетей L2. Такие туннели могут быть установлены поверх любого IP-транспорта, включая другие VPN, такие как IPsec или OpenVPN, что обеспечивает гибкий способ безопасного расширения связности на 2-м уровне.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
local-ip **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
tunnel-ip **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
tunnel-id **минимум:** 1, **максимум:** 65535	ID туннеля
macaddr **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
mtu **минимум:** 70, **максимум:** 65535	MTU интерфейса
ttl **минимум:** 1, **максимум:** 255	TTL интерфейса
dscp	DSCP метка, присваемая GRE трафику

encryption **значения:** none	Метод защиты туннеля
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec

13.2. gre

Данный раздел настраивает туннели GRE (Generic Routing Encapsulation) — универсальный протокол для инкапсуляции широкого спектра протоколов сетевого уровня внутрь IP-туннелей типа "точка-точка".

Основное преимущество GRE заключается в его способности транспортировать данные, которые не могут быть напрямую маршрутизированы в стандартной IP-сети, например, не-IP протоколы или multicast-трафик. Он также часто используется для создания оверлейных сетей, например, для передачи трафика IPv6 через сеть, работающую только на IPv4 (и наоборот).

Эта страница позволяет настроить все стандартные параметры GRE, включая конечные точки туннеля (*Local IP* и *Remote IP*) и опциональный *Ключ* для идентификации конкретного туннеля при наличии нескольких соединений с одним удаленным узлом. Также здесь доступны расширенные средства управления пакетами, такие как изменение *TTL* и *ToS*, и встроенный механизм *Keepalive* для мониторинга состояния туннеля и его автоматического отключения, если удаленная точка становится недоступной.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
local-ip **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
tunnel-ip **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
key **минимум:** 0, **максимум:** 4294967295	GRE key туннеля
encryption **значения:** none	Метод защиты туннеля
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
mtu **минимум:** 70, **максимум:** 65535	MTU туннельного интерфейса
ttl **минимум:** 1, **максимум:** 255	TTL туннельного интерфейса
dscp	DSCP метка, присваемая GRE трафику
do-not-frag **значения:** true, false	Установить флаг запрета фрагментации пакета

keepalive-delay **минимум:** 0, **максимум:** 4294967	Интервал отправки keepalive пакета в отсутствии трафика в туннеле
keepalive-retries **минимум:** 0, **максимум:** 4294967295	Число попыток до перехода в состояние DOWN **условия:** keepalive-delay != "" && keepalive-delay != 0

13.3. ipsec

13.3.1. association

В этом разделе определяются ключевые политики безопасности IPsec. Эти политики, часто именуемые дочерними SA (Child SA) в терминологии IKEv2, являются правилами, которые точно устанавливают, какой сетевой трафик подлежит защите, как он будет защищен, и между какими узлами.

Основная функция здесь — это настройка *Локальных* и *Удаленных селекторов трафика*. Эти селекторы определяют "целевой трафик", который будет инициировать инкапсуляцию IPsec. Указывая диапазоны IP-адресов, протоколы и порты, можно создавать точные правила, соответствующие требованиям безопасности вашей сети.

Каждая политика привязывается к определенному *Соединению* (которое определяет пиры) и использует *Профиль* (который определяет алгоритмы шифрования и целостности для Фазы 2), что создает модульную и масштабируемую конфигурацию.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, что позволяет добавлять или изменять политики без разрыва существующих, активных безопасных ассоциаций. Для принудительного закрытия конкретной SA используйте страницу Status.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
connection	IKE соединение для согласования SA
proposal **значения:** /tunnel ipsec proposal	Алгоритм шифрования и аутентификации ESP
auto **значения:** route, start	Действие после применения конфигурации SA
type **значения:** tunnel, transport, passthrough, drop	Согласование режима работы SA
leftsubnet	Источники трафика для согласования с локальной стороны
rightsubnet	Источники трафика для согласования с удалённой стороны

13.3.2. connection

В этом разделе определяются соединения IKE (Internet Key Exchange). Соединение IKE устанавливает идентификационные данные и параметры безопасности для самих пиров, создавая защищенный канал управления (SA Фазы 1), который используется для согласования политик шифрования данных (дочерних SA Фазы 2).

Ключевые настройки включают:

- Определение пиров путем указания их *локального* и *удаленного* адресов шлюзов.
- Выбор версии IKE (*IKEv1* или *IKEv2*), которая будет управлять процессом согласования.
- Указание идентификаторов пиров (*Local ID*, *Remote ID*) и метода аутентификации (*Local auth*, *Remote auth*). Это ядро модели безопасности, поддерживающее такие методы, как общие ключи (Pre-Shared Keys, PSK) и аутентификацию по открытым ключам (на основе сертификатов).
- Назначение профиля IKE, который содержит конкретные алгоритмы шифрования и целостности Фазы 1, используемые для защиты канала управления.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, что позволяет добавлять или изменять политики без разрыва существующих, активных безопасных ассоциаций. Для принудительного закрытия конкретной SA используйте страницу Status.

СВОЙСТВА

left **значения:** /ip interface, /mobile modem, auto	Локальный адрес туннеля или интерфейс
right **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
keyexchange **значения:** ikev2, ikev1	Версия протокола IKE для безопасного согласования SA
profile **значения:** /tunnel ipsec profile	IKE/ISAKMP профиль шифрования и аутентификации SA
leftid	Локальный IKE идентификатор для аутентификации **условия:** auth = pubkey
rightid	IKE идентификатор для аутентификации удалённой стороны
auth **значения:** psk, pubkey	Метод аутентификации между сторонами
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** auth = psk
cert **значения:** /storage certificate	Сертификат (включая закрытый ключ) **условия:** auth = pubkey
leftsourceip **пример:** 192.168.1.1, %config	Virtual IP для использования в качестве источника трафика
rightsourceip **пример:** 192.168.1.1/24, 192.168.1.1-192.168.1.100, %config	Выделить виртуальный адрес для удалённой стороны

13.3.3. profile

В этом разделе определяются многоразовые **Профили IKE**. Каждый профиль представляет собой именованный набор криптографических алгоритмов и параметров, который управляет процессом установления безопасной ассоциации Фазы 1 (IKE SA).

Создание таких профилей позволяет стандартизировать и упростить конфигурацию IPsec. Вместо того чтобы повторно определять один и тот же набор алгоритмов для каждого соединения, можно

создать один профиль и ссылаться на него из нескольких *Соединений* IKE.

Профиль определяет все ключевые параметры безопасности для согласования IKE, включая:

- Разрешенные алгоритмы *Шифрования*, *Хеширования* и *Псевдослучайной функции*.
- *Группу Диффи-Хеллмана (DH)*, используемую для безопасного обмена ключами.
- *Время жизни IKE*, которое определяет, как долго SA Фазы 1 остается действительной, прежде чем потребуется повторное согласование.
- Параметры Dead Peer Detection (*DPD*), которые контролируют, как роутер отслеживает доступность удаленного пира и какое *Действие* предпринимать, если пир перестает отвечать.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, что позволяет добавлять или изменять политики без разрыва существующих, активных безопасных ассоциаций. Для принудительного закрытия конкретной SA используйте страницу Status.

СВОЙСТВА

encryption **значения:** aes128, aes192, aes256, 3des	Алгоритм шифрования для безопасной передачи данных
hash **значения:** sha1, sha256, sha384, sha512, md5	Хэш-функция проверки подлинности
prf **значения:** sha1, sha256, sha384, sha512, md5	Псевдослучайная хэш-функция для получения материала ключа
dh **значения:** modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192	Протокол Diffie-Hellman для обмена ключами
ikelifetime	Интервал времени до пересогласования IKE/ISAKMP SA
dpddelay	Интервал отправки DPD пакета (если нет иного трафика)
dpdtimeout	Таймаут без ответа на DPD пакет, через который прервать IKEv1 соединение
dpdaction **значения:** hold, restart, clear, none	Действие, выполняемое при разрыве соединения по таймауту

13.3.4. proposal

В этом разделе определяются многоразовые **Профили IPsec (Proposals)**. Каждый профиль представляет собой именованный набор алгоритмов безопасности, который управляет тем, как именно будет защищаться трафик данных внутри IPsec-туннеля (SA Фазы 2, или дочерняя SA).

Аналогично Профилям IKE, эти профили обеспечивают модульный подход к управлению политиками безопасности. Определяя профиль, вы задаете набор алгоритмов *Шифрования* и *Аутентификации*, которые будут использоваться протоколом ESP (Encapsulating Security Payload) для обеспечения конфиденциальности и целостности данных.

Ключевые параметры, определяемые в профиле, включают:

- Криптографические алгоритмы для защиты данных (*Шифрование*, *Аутентификация*).
- Группу Perfect Forward Secrecy (*PFS*), которая гарантирует, что для каждого сеанса будет сгенерирован новый, независимый ключ, что повышает долгосрочную безопасность.

- *Время жизни* дочерней SA, которое определяет, как часто должны пересогласовываться ключи шифрования данных.

Эти профили затем используются в разделе "Associations", чтобы легко применять одинаковые политики защиты данных к разным туннелям.

СВОЙСТВА

encryption **значения:** aes128, aes192, aes256, 3des	Алгоритм шифрования для безопасной передачи данных
auth **значения:** sha1, sha256, sha384, sha512, md5	HMAC алгоритм для аутентификации
pfs **значения:** modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, none	Алгоритм PFS, гарантирует что DH ключи не будут использованы повторно
lifetime	Интервал времени (сек) до пересогласования

13.3.5. status

Данный раздел отображает текущее рабочее состояние всех настроенных IPsec-туннелей. Он служит основным диагностическим инструментом для проверки активности настроенных туннелей и для устранения проблем с подключением.

Страница наглядно показывает результат настроек, заданных в разделах *Connections* и *Associations*. Здесь администратор может убедиться, что нужные пиры (*LOCAL-ID* и *REMOTE-ID*) и политики трафика (*LOCAL-TS* и *REMOTE-TS*) успешно согласовали и установили туннель.

Столбец *STATUS* особенно полезен для диагностики, поскольку он предоставляет конкретную информацию о состоянии туннеля, что позволяет быстро выявлять проблемы конфигурации или сети. Таблица также содержит важные операционные данные, включая время работы туннеля и счетчики трафика.

КОМАНДЫ

debug	Изменить уровень детализации логгирования level - Уровень детализации логирования (обязательно)

СВОЙСТВА

association	IPSec SA **условия:** association != ""
uniqueid	Уникальный идентификатор SA
status	Статус SA
local	Адрес с которого строится туннель
local-id	Локальной IKE идентификатор
remote	Адрес на который строится туннель
remote-id	IKE идентификатор удалённой стороны
uptime	Время с момента установки SA
encryption	Согласованый алгоритм шифрования
integrity	Согласованый алгоритм проверки целостности

prf	Согласованый PRF алгоритм
dh	Согласованая группа DH
local-ts	Источник трафика с локальной стороны
remote-ts	Источник трафика с удалённой стороны
expires	Время до истечения SA (rekeying/reauthentication)
reqid	Уникальный номер SA
rx-tx	Счётчик полученного / отправленного трафика

13.4. l2tp

Данный раздел настраивает роутер для работы в качестве клиента L2TPv2, позволяя ему устанавливать безопасный туннель с удаленным L2TP-сервером. Туннель устанавливается поверх протокола PPP (Point-to-Point Protocol) и обычно используется для подключения к корпоративным сетям или сервисам удаленного доступа.

Основная настройка включает в себя указание *IP-адреса* удаленного сервера и предоставление необходимых *Имени пользователя* и *Пароля* для аутентификации. *Тип аутентификации* можно выбрать в соответствии с требованиями сервера.

Помимо базовой настройки подключения, можно включить *Шифрование* (как правило, MPPE) для защиты передаваемых данных. Поле *Метрика* позволяет управлять приоритетом маршрута в таблице маршрутизации роутера, что является важным для конфигураций с несколькими WAN-каналами или для отказоустойчивости.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
local-ip **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN или IP адрес)
username	Имя пользователя
password	Пароль пользователя
auth **значения:** any, chap, mschap, mschap-v2, pap	Выбор протокола для аутентификации **условия:** encryption = mppe
encryption **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point

debug **значения:** true, false	Режим подробного логгирования

13.5. l2tp v3

В этом разделе настраиваются туннели L2TPv3 (Layer 2 Tunneling Protocol version 3) — стандартизированный IETF протокол для создания соединений 2-го уровня "точка-точка" поверх IP-сети.

В отличие от своего предшественника L2TPv2, протокол L2TPv3 работает независимо от PPP и разработан как более универсальный и эффективный механизм транспорта L2. Его основная функция — инкапсулировать и передавать полные Ethernet-кадры, фактически создавая «псевдо-провод», который соединяет два удаленных сетевых сегмента.

Настройка требует определения конечных точек туннеля (*Local IP*, *Remote IP*) и набора уникальных идентификаторов (*Tunnel-Id*, *Session-Id*), которые должны совпадать на обеих сторонах для установки соединения.

L2TPv3 не имеет собственного встроенного шифрования, для защиты он использует нижележащий протокол безопасности транспортного уровня. Данная реализация поддерживает включение *IPsec* для шифрования всего туннеля L2TPv3.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
local-ip **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tpv3, /tunnel atunnel, /defaults server, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
tunnel-ip **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
encryption **значения:** none	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
macaddr **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
mtu **минимум:** 70, **максимум:** 65535	MTU интерфейса
l2spec-type **значения:** default, none	Тип заголовка (header) для второго уровня
tunnel-id **минимум:** 1, **максимум:** 4294967295	ID туннеля
peer-tunnel-id **минимум:** 1, **максимум:** 4294967295	ID туннеля удалённой стороны

session-id **минимум:** 1, **максимум:** 4294967295	ID сессии туннеля
peer-session-id **минимум:** 1, **максимум:** 4294967295	ID сессии удалённой стороны
encap **значения:** ip, udp	Тип инкапсуляции протокола
udp-dport **минимум:** 1024 **пример:** 80, !80	UDP порт удалённой стороны в случае UDP энкапсуляции **условия:** encap = udp
udp-sport **минимум:** 1024 **пример:** 80, !80	UDP порт для UDP энкапсуляции **условия:** encap = udp

13.6. openvpn

Данный раздел настраивает клиент OpenVPN — универсальный и высокозащищенный VPN-протокол с открытым исходным кодом. OpenVPN широко используется для создания как site-to-site, так и удаленных VPN-подключений путем установления зашифрованного туннеля через публичную сеть.

Модель безопасности OpenVPN построена на протоколе SSL/TLS, используя сертификаты и закрытые ключи для надежной аутентификации и обмена ключами. Его гибкость позволяет работать как поверх *UDP* (предпочтительно для производительности), так и *TCP* (для надежности и обхода ограничивающих межсетевых экранов).

Конфигурация на этой странице позволяет определить все аспекты клиентского подключения:

- Тип виртуального интерфейса: *TUN* для маршрутизируемого IP-туннеля 3-го уровня или *TAP* для Ethernet-туннеля 2-го уровня (сетевой мост).
- Адрес удаленного сервера и транспортный *протокол*.
- Требуемые криптографические параметры, включая алгоритмы *Шифрования* и *Аутентификации*.
- Необходимые учетные данные безопасности, такие как сертификат *Центра Сертификации (CA)*, *Сертификат* клиента и его закрытый ключ. Для некоторых конфигураций также могут использоваться *Имя пользователя*/*Пароль* или статический ключ *TLS-Auth*.

КОМАНДЫ

generate-ta-key	Сгенерировать файл случайного ключа, используемый как TA Key или Static Key filename - Имя конфигурации (обязательно)

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
local-ip **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tp-v3, /tunnel atunnel, /defaults server, auto **пример:** bridge0	Локальный адрес туннеля или интерфейс
remote-ip	Адрес удалённого хоста (FQDN ил IP адрес)

tunnel-ip **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
dev-type **значения:** tun, tap	Тип виртуального интерфейса
protocol **значения:** tcp, udp	Транспортный протокол туннеля
encryption **значения:** none, tls, static-key	Метод шифрования туннеля
static-key **значения:** /storage file	PSK файл для шифрования статическим ключем **условия:** encryption = static-key
cipher **значения:** AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-192-GCM, AES-256-CBC, AES-256-GCM	Алгоритм шифрования туннеля **условия:** encryption = tls encryption = static-key
auth **значения:** MD5, SHA1, SHA256, SHA384, SHA512, none	HMAC алгоритм для аутентификации **условия:** encryption = tls encryption = static-key
ta-key **значения:** /storage file	Ключ дополнительной HMAC аутентификации **условия:** encryption = tls
ca **значения:** /storage certificate	Публичный ключ удостоверяющего цетра (CA) **условия:** encryption = tls
cert **значения:** /storage certificate	Локальный сертификат (включая приватный ключ) **условия:** encryption = tls
username	Имя пользователя для аутентификации **условия:** encryption = tls
password	Пароль пользователя для аутентификации **условия:** encryption = tls
flag **значения:** allow-recursive-routing, auth-nocache, auth-user-pass-optional, client-to-client, comp-noadapt, fast-io, float, mtu-test, multihome, ncp-disable, nobind, opt-verify, passtos, persist-key, persist-local-ip, persist-remote-ip, persist-tun, ping-timer-rem, pull, push-peer-info, push-reset, remote-random, route-nopull, single-session, suppress-timestamps, tcp-nodelay, tls-client, tls-exit, tls-server, username-as-common-name	Дополнительные опции туннеля
extra **значения:** auth-retry, bcast-buffers, comp-lzo, compress, connect-freq, connect-retry, connect-retry-max, connect-timeout, ecdh-curve, explicit-exit-notify, fragment, hand-window, hash-size, ifconfig_local, ifconfig_remote, ifconfig_netmask, ifconfig-push-local, ifconfig-push-netmask, inactive, key-direction, keysize, link-mtu, lport, max-clients, mssfix, mtu-disc, ping, ping-exit, ping-restart, prng, pull-filter-accept, pull-filter-ignore, pull-filter-reject, rcvbuf, remote-cert-tls, reneg-bytes, reneg-pkts, reneg-sec, replay-persist, replay-window, resolv-retry, shaper, sndbuf, topology, tcp-queue-limit, tls-timeout, tls-version-min, tran-window, tun-mtu, tun-mtu-extra, txqueuelen, verb, verify-client-cert, verify-x509-name, x509-username-field	Дополнительные параметры туннеля

13.7. pptp

Данный раздел настраивает роутер для работы в качестве клиента PPTP (Point-to-Point Tunneling Protocol). Это позволяет роутеру устанавливать VPN-туннель с удаленным PPTP-сервером, как правило, для удаленного доступа к частной сети.

PPTP — это широко поддерживаемый, но устаревший VPN-протокол. Его настройка проста и в основном требует указания *IP-адреса* удаленного сервера, а также *Имени пользователя* и *Пароля* для аутентификации.

Страница конфигурации позволяет выбрать *Тип аутентификации* (например, MS-CHAPv2) и включить *Шифрование* (MPPE) для обеспечения базового уровня конфиденциальности данных.

PPTP является устаревшим протоколом с известными уязвимостями в безопасности. Его использование категорически не рекомендуется для любых приложений, где важна безопасность данных. Для безопасного удаленного доступа рекомендуется использовать современные VPN-протоколы, такие как IPsec или OpenVPN.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
local-ip **значения:** /ip interface, /mobile modem, /tunnel eoip, /tunnel gre, /tunnel l2tp, /tunnel openvpn, /tunnel pptp, /tunnel wireguard interface, /tunnel l2tp-v3, /tunnel atunnel, /defaults server, auto **пример:** bridge0	Локальный адрес туннеля или интерфейс
remote-ip **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
username	Имя пользователя
password	Пароль пользователя
auth **значения:** any, chap, mschap, mschap-v2, pap, eap	Выбор протокола для аутентификации **условия:** encryption = mppe
encryption **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point
debug **значения:** true, false	Режим подробного логгирования

13.8. wireguard

13.8.1. interface

Данный раздел предназначен для настройки локального сетевого интерфейса WireGuard. Этот интерфейс выступает в роли одной из конечных точек защищенного туннеля, и его идентификация определяется в первую очередь парой криптографических ключей. В WireGuard именно *Публичный ключ* служит единственным идентификатором интерфейса, заменяя собой традиционные имена пользователей или сложные сертификаты.

Основная настройка включает в себя генерацию *Приватного ключа* (из которого вычисляется публичный ключ) и назначение уникального *IP-адреса* в пределах виртуальной сети VPN. Кроме того, здесь определяется *Порт* для прослушивания входящих подключений от пиров.

Настройка этого интерфейса — это только первый шаг. Для создания рабочего туннеля необходимо перейти в раздел *Peer* и определить удаленные узлы, которым разрешено подключаться к этому интерфейсу.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
tunnel-ip **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
priv-key **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Приватный ключ для аутентификации и шифрования трафика
pub-key **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Публичный ключ для аутентификации и шифрования трафика
port **пример:** 22, 51820	Порт для входящих подключений
mtu **минимум:** 70, **максимум:** 65535	MTU интерфейса
fw-mark	Установить метку для пакетов, ассоциированных с этим интерфейсом

13.8.2. peer

В этом разделе определяются удаленные узлы (пиры), которым разрешено подключаться к локальному интерфейсу WireGuard. Пир представляет собой одну удаленную конечную точку в VPN-туннеле.

Настройка пира выполняет две критически важные, одновременные функции: **аутентификацию** и **маршрутизацию**.

- **Аутентификация:** Пир в первую очередь идентифицируется по своему *Публичному ключу*. Только тот узел, который сможет доказать владение соответствующим приватным ключом, сможет установить соединение. Опционально можно добавить *Общий ключ (Preshared Key)* для дополнительного уровня безопасности на основе симметричного ключа.

- **Маршрутизация:** Список *Разрешенных IP-адресов* — это фундаментальная концепция в WireGuard. Он определяет, какие IP-адреса "принадлежат" данному пиру. Любой трафик, отправленный из туннеля с IP-адресом источника из этого списка, будет принят. И наоборот, любой трафик, отправленный в туннель и предназначенный для адреса из этого списка, будет автоматически зашифрован и направлен именно этому пиру.

Опционально можно настроить интервал *Keepalive* для поддержания постоянного соединения через межсетевые экраны с отслеживанием состояний и устройства NAT.

КОМАНДЫ

generate-psk	Сгенерировать и добавить PSK ключ

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
interface **значения:** /tunnel wireguard interface	Сетевой интерфейс Wireguard
remote-ip **пример:** example.com:80, 192.168.1.1:80	Адрес удалённого хоста (IP адрес и порт)
allowed-ip	Адрес, ассоциированный с этим Peer для обеспечения маршрутизации
pub-key **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Публичный ключ для аутентификации и шифрования трафика
psk **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Дополнительный ключ для увеличения безопасности
keepalive **минимум:** 0, **максимум:** 65535	Интервал (сек) отправки keepalive пакета

14. wireless

14.1. adapter

Данный раздел предназначен для низкоуровневой настройки физических Wi-Fi-адаптеров, установленных в роутере. Настройки здесь определяют базовые рабочие параметры самого оборудования, напрямую управляя его поведением в радиоэфире и обеспечивая соответствие нормативным требованиям.

Настройка на этом уровне включает в себя установку ограничений, специфичных для страны, выбор доступных каналов и определение мощности передачи. Это первоначальный этап настройки и необходимое условие для создания одной или нескольких виртуальных точек доступа, которые будут транслировать SSID сетей.

КОМАНДЫ

scan	Поиск WiFi сетей

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
country **значения:** AD, AE, AF, AI, AL, AM, AN, AR, AS, AT, AU, AW, AZ, BA, BB, BD, BE, BF, BG, BH, BL, BM, BN, BO, BR, BS, BT, BY, BZ, CA, CF, CH, CI, CL, CN, CO, CR, CU, CX, CY, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, ET, FI, FM, FR, GB, GD, GE, GF, GH, GL, GP, GR, GT, GU, GY, HK, HN, HR, HT, HU, ID, IE, IL, IN, IR, IS, IT, JM, JO, JP, KE, KH, KN, KP, KR, KW, KY, KZ, LB, LC, LI, LK, LS, LT, LU, LV, MA, MC, MD, ME, MF, MH, MK, MN, MO, MP, MQ, MR, MT, MU, MV, MW, MX, MY, NG, NI, NL, NO, NP, NZ, OM, PA, PE, PF, PG, PH, PK, PL, PM, PR, PT, PW, PY, QA, RE, RO, RS, RU, RW, SA, SE, SG, SI, SK, SN, SR, SV, SY, TC, TD, TG, TH, TN, TR, TT, TW, TZ, UA, UG, US, UY, UZ, VC, VE, VI, VN, VU, WF, WS, YE, YT, ZA, ZW, default	Выбор страны для применения регуляторных ограничений
channels **значения:** $_channels	Список WiFi каналов для работы адаптера
txpower **значения:** auto, $_txpowers	Мощность исходящего сигнала
htmode **значения:** none, $_htmodes	Режим повышенной производительности, определяющий ширину канала
frag-threshold **минимум:** 256, **максимум:** 2346	Размер (байт) посылки, превышение которого ведёт к его фрагментации
rts-threshold **минимум:** 0, **максимум:** 2347	Размер (байт) посылки, после превышения которого включается механизм RTS/CTS
beacon **минимум:** 15, **максимум:** 65535	Интервал (мсек) отправки AP beacon

14.2. filter

Данный раздел предназначен для настройки списков контроля доступа (ACL) на основе MAC-адресов для беспроводных сетей. Эта функция обеспечивает дополнительный уровень безопасности, ограничивая доступ к сети только авторизованным устройствам.

Система реализует модель «белого списка» (whitelist). Это означает, что когда фильтр применяется к беспроводной сети, подключаться смогут только те клиентские устройства, MAC-адреса которых присутствуют в списке. Всем остальным устройствам доступ будет запрещен.

На этой странице создаются и управляются сами списки фильтров. Непосредственное применение фильтра к конкретной беспроводной сети выполняется в разделе *Wireless/Network*.

СВОЙСТВА

mac	MAC адрес WiFi устройства

14.3. network

В этом разделе определяются логические беспроводные сети, каждая из которых работает поверх физического *Адаптера*. Каждая настроенная здесь сеть представляет собой отдельный беспроводной сервис, такой как Точка Доступа (AP), транслирующая SSID, клиент, подключающийся к вышестоящей Wi-Fi сети, или узел в mesh-сети.

Режимы работы

Ключевым выбором конфигурации является *Режим* работы, который определяет роль данной беспроводной сети:

- **Точка доступа (ap):** Наиболее распространенный режим. Роутер транслирует *SSID*, к которому могут подключаться клиентские устройства.
- **Клиент (sta):** Режим клиента. Роутер подключается к другой существующей Wi-Fi сети, обычно для использования ее в качестве WAN-канала или для объединения сетей.
- **Узел mesh-сети (mesh):** Специализированный режим для построения распределенной, самовосстанавливающейся mesh-сети с другими совместимыми устройствами.

Безопасность и контроль доступа

Помимо определения режима, здесь настраиваются основные параметры безопасности и контроля доступа для каждой сети:

- **Аутентификация:** Определение профиля безопасности путем выбора типа *Шифрования* (например, WPA2/WPA3) и установки *Ключа* сети.
- **Контроль доступа:** Применение политики *MAC-фильтрации* путем выбора заранее созданного списка из раздела *Беспроводная связь / MAC-фильтр*.
- **Изоляция клиентов:** В режиме *ap* включение *Изоляции клиентов* запрещает беспроводным устройствам, подключенным к одному SSID, напрямую обмениваться данными друг с другом.

СВОЙСТВА

disabled **значения:** true, false	Выключить конфигурацию
adapter **значения:** /wireless adapter	WiFi адаптер
mode **значения:** ap, sta, mesh	Режим работы в беспроводной WiFi сети
encryption **значения:** none, psk-mixed+ccmp, wpa-mixed+ccmp, sae	Тип шифрования данных в беспроводной WiFi сети **условия:** mode = mesh
ssid	Имя беспроводной WiFi сети для её идентификации в эфире
key **мин. длина:** 8	Пароль аутентификации в беспроводной WiFi сети **условия:** encryption = psk-mixed+ccmp encryption = sae
wds **значения:** true, false	Use 4-address mode to allow transparent ethernet bridging **условия:** mode != mesh
wmm **значения:** true, false	WiFi Multimedia Mode включает механизм QoS для мультимедиа трафика
mesh-forward **значения:** true, false	Пересылать пакеты не предназначенные для этой mesh станции **условия:** mode = mesh

mesh-ttl	Количество прыжков, которые пакет может пройти внутри mesh сети **условия:** mode = mesh
mesh-rssi-threshold **минимум:** -100, **максимум:** 1	Требование минимального RSSI необходимого для поддержания связи внутри mesh сети **условия:** mode = mesh
hidden **значения:** true, false	Отключить вещание beacon **условия:** mode = ap
mtu **минимум:** 256, **максимум:** 2304	MTU интерфейса
isolate **значения:** true, false	Запретить клиентам коммуницировать друг с другом **условия:** mode = ap
mac-filter **значения:** deny, allow, disable	Политика ACL для фильтрации беспроводных устройств **условия:** mode = ap && encryption != wpa-mixed+ccmp
mac-list **значения:** /wireless filter	ACL беспроводных устройств **условия:** mode = ap && mac-filter != disable && mac-filter != radius && encryption != wpa-mixed+ccmp
auth-server **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес сервера аутентификации **условия:** mac-filter = radius encryption = wpa-mixed+ccmp && mode != sta
auth-secret	Общий ключ сервре аутентификации **условия:** mac-filter = radius encryption = wpa-mixed+ccmp && mode != sta
eap-method **значения:** peap, tls, ttls	EAP authentication method **условия:** mode = sta && encryption = wpa-mixed+ccmp
eap-auth-method **значения:** pap, mschap-v2	WPA/WPA2 enterprise authentication method **условия:** encryption = wpa-mixed+ccmp && mode = sta && eap-protocol = ttls encryption = wpa-mixed+ccmp && mode = sta && eap-protocol = peap
eap-username **пример:** bridge0, vpn, client_1	Логин пользователя для аутентификации WPA/WPA2 Enterprise **условия:** encryption = wpa-mixed+ccmp && mode = sta
eap-password	Пароль пользователя для аутентификации WPA/WPA2 Enterprise **условия:** encryption = wpa-mixed+ccmp && mode = sta
ca **значения:** /storage certificate	CA сертификат **условия:** encryption = wpa-mixed+ccmp && mode = sta
cert **значения:** /storage certificate	Сертификат для аутентификации **условия:** encryption = wpa-mixed+ccmp && mode = sta