Настройка VPN-сервера UserGate (L2TP)

Настройка серверной части UserGate состоит из нескольких шагов и реализует функцию единой транзитной точки агрегации трафика для всех клиентских установок UserGate.

Шаг 1. Создать локальных VPN-пользователей и профиль авторизации

Для проверки подлинности VPN-подключений от клиентских установок UserGate необходимо задать отдельные учетные записи для аутентификации данных подключений и сформировать их них отдельную группу пользователей для будущей VPN-топологии. Рекомендуется использовать различные имена пользователей и пароли для каждой из клиентский установок UserGate. Профиль авторизации необходим для указания метода аутентификации пользователей в серверном VPN-правиле.

Создание локального пользователя:

1. В разделе Пользователи и устройства → Пользователи нажмите Добавить.
2. На вкладке Общие включите опцию Включено и задайте имя пользователя (обычно используется название филиала организации) и пароль для аутентификации каждого клиентского VPN-соединения.
3. Нажмите Сохранить.

После создания пользовательских учетных данных необходимо сформировать из них отдельную группу пользователей для VPN-подключений:

1. В разделе Пользователи и устройства → Группы нажмите Добавить.
2. На вкладке Свойства локальной группы введите название группы и ее описание.
3. В разделе Пользователи нажмите Добавить и укажите все учетные записи, предназначенные для VPN-подключений.
4. Нажмите Сохранить.

Для создания профиля авторизации:

1. Перейдите в раздел Пользователи и устройства → Профили авторизации.
2. Нажмите Добавить.
3. На вкладке Общие введите название и описание профиля.
4. На вкладке Методы аутентификации нажмите Добавить и выберите Локальный пользователь.
5. Нажмите Сохранить.

Шаг 2. Создать VPN-зону

Необходимо создать новую зону с выделенной IP-адресацией. Она станет транзитной подсетью, через которую будет передаваться трафик между всеми участниками VPN-соединения.

Для создания VPN-зоны:

1. Перейдите в раздел Сеть → Зоны.
2. Нажмите Добавить.
3. На вкладке Общие введите название и описание новой зоны.
4. На вкладке Контроль доступа выберите пункты ICMP и VPN.
5. Нажмите Сохранить.

Шаг 3. Создать разрешающее правило межсетевого экрана для VPN-трафика

Для передачи VPN-трафика необходимо создать отдельное правило, в котором должны одновременно фигурировать в качестве источника и назначения внутренние локальные зоны и VPN-зона. Это позволит реализовать свободное межсетевое взаимодействие по туннелю в обоих направлениях.

Для создания разрешающего правила для VPN-трафика:

1. В разделе Политики сети → Межсетевой экран нажмите Добавить.
2. Задайте название и описание правила. В пункте Действие установите значение Разрешить.
3. На вкладках Источник и Назначение задайте VPN-зону и внутренние зоны, доступ к которым должен быть реализован через VPN-соединение.
4. Нажмите Сохранить.

Шаг 4. Создать профиль безопасности VPN

Профиль безопасности VPN определяет такие настройки, как общий ключ шифрования (Preshared key) и алгоритмы шифрования. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с различными параметрами безопасности.

Создание профиля VPN:

1. Перейдите в раздел VPN → Профили безопасности VPN.
2. Нажмите Добавить для создания нового профиля безопасности.
3. На вкладке Общие введите название и описание профиля. Далее укажите параметры работы IKE в соответствующих строках.
4. В разделе Общий ключ введите ключ шифрования, который должен совпадать у всех участников VPN-сети. Ключ шифрования должен состоять из сложных комбинаций букв, цифр и символов и иметь длину не менее 8 символов.
5. На вкладке Фаза 1 при необходимости укажите время жизни ключа шифрования (параметр Время жизни ключа), интервал определения недоступных участников VPN-сети (параметр Интервал Dead Peer detection) и количество неудачных попыток подключения (параметр Неудачные попытки), при достижении которого UserGate выдаст сообщение об ошибке подключения.

6. В разделе Diffie-Hellmann группы укажите те группы, которые поддерживаются на стороне клиентов VPN-подключений. Рекомендуемые группы: 2, 5, 14, 15, 16.
7. В разделе Безопасность удалите существующие записи. Выберите алгоритм авторизации не ниже SHA256 и шифрования не ниже AES128. Если параметров не видно в интерфейсе, потяните мышью нижнюю синюю рамку окна настроек.
8. На вкладке Фаза 2 при необходимости укажите время жизни ключа шифрования (параметр Время жизни ключа) и максимальный объем данных, которые можно зашифровать одним ключом (параметр Максимальный объем данных, шифруемых одним ключом). Смена ключа произойдет автоматически при достижении заданного объема переданного трафика.
9. В разделе Безопасность выберите алгоритм авторизации не ниже SHA256 и шифрования не ниже AES128.
10. Дважды нажмите Сохранить.

Шаг 5. Создать VPN-интерфейс

VPN-интерфейс — это виртуальный сетевой адаптер, который используется для построения транзитной виртуальной VPN-сети. Для масштабирования VPN-сети рекомендуется задать для VPN-зоны внутреннюю подсеть с маской /24, что позволит объединить до 254 удаленных площадок.

Предупреждение

Подсеть этого интерфейса является виртуальной и существует только между устройствами UserGate. Ее не нужно назначать на виртуальном коммутаторе каждого VDC.

Создание туннельного VPN-интерфейса:

1. В разделе Сеть → Интерфейсы выберите зону, которая имеет выход в интернет, чтобы разрешить работу VPN-соединений.

2. Нажмите Редактировать и во всплывающем окне Свойства сетевой зоны на вкладке Контроль доступа включите опцию VPN и сохраните настройки.
3. В разделе Сеть →Интерфейсы нажмите Добавить и выберите Добавить VPN.
4. На вкладке Общие окна Настройка VPN адаптера активируйте параметр Включено.
5. В пункте Название введите номер интерфейса, начания с 4. Это локальный идентификатор VPN-интерфейса “tunnel4”.
6. В пункте Зона выберите VPN-зону, которая была создана на Шаге 2.
7. На вкладке Сеть установите режим адресации «Статический» для VPN-интерфейса.
8. В разделе IP интерфейса нажмите Добавить и введите необходимую адресацию подсети с маской /24. Конечный IP-адрес туннельного интерфейса установите по аналогии со шлюзом по умолчанию: 1 или 254.
9. Дважды нажмите Сохранить.

Шаг 6. Создать сети VPN

Сеть VPN определяет диапазоны адресов, которые будут анонсированы при подключении к VPN-серверу клиентских установок BM UserGate. Таким образом клиент UserGate будет обладать информацией, что данные подсети находятся именно в VPN-сети. Обычно в VPN-сети добавляются конечные подсети на удаленной стороне, между которыми необходимо обеспечить межсетевое взаимодействие.

Создание сети VPN:

1. Перейдите в раздел VPN →Сети VPN, нажмите Добавить.
2. В появившемся окне Свойства VPN-сети на вкладке Общие введите название и описание создаваемой VPN-сети.
3. На вкладке Сеть укажите адресуемый диапазон внутри туннельного интерфейса, совпадающий с тем диапазоном, который был указан на Шаге 5. Формат записи IP-адреса: ..*.A-..*.B.
4. На вкладке Маршруты нажмите Добавить –> IP-адрес и введите диапазоны внутренних подсетей, которые должны передаваться клиентской BM UserGate и взаимодействие с которыми будет происходить через VPN-туннель.

5. Нажмите Сохранить.

Шаг 7. Создать маршруты VPN

Чтобы VPN-сервер имел информацию об IP-подсетях, которые расположены за каждым из VPN-клиентов, необходимо прописать соответствующие статические маршруты на сервере, указав в качестве адресов назначения адреса удаленных клиентских ВМ UserGate внутри VPN-туннеля.

1. Перейдите в раздел Сеть → Виртуальные маршрутизаторы, выберите стандартный контекст маршрутизатора Виртуальный маршрутизатор по умолчанию и нажмите Редактировать.
2. В появившемся окне Свойства виртуального маршрутизатора из раскрывающегося списка выберите Статические маршруты и нажмите Добавить.
3. В появившемся окне Свойства маршрута активируйте опцию Включено. Введите название и описание маршрута для указания сетей, находящийся за IP-адресом удаленного VPN-клиента UserGate.
4. В пункте Адрес назначения укажите IP-адреса или группы адресов внутренних подсетей, которые расположены за удаленной клиентской ВМ UserGate. Пример записи: 10.20.0.0/16.
5. В пункте Шлюз укажите IP-адрес внутреннего туннельного VPN-интерфейса удаленного UserGate.
6. В пункте Интерфейс выберите VPN-интерфейс “tunnel4”, который был создан на Шаге 5.
7. Дважды нажмите Сохранить.

Шаг 8. Создать серверное правило VPN

Серверное правило VPN повторяет логику работы политики межсетевого взаимодействия. В нем должны быть указаны исходные зоны источника VPN-трафика и параметры конфигурации, которые были созданы выше.

Создание серверного правила VPN:

1. Перейдите в раздел VPN → Серверные правила и нажмите Добавить.
2. В появившемся окне Свойства активируйте опцию Включено и задайте название правила на латинице и его описание при необходимости.
3. В полях Профиль безопасности VPN, Сеть VPN, Профиль авторизации и Интерфейс выберите элементы, которые были созданы на предыдущих этапах.
4. На вкладках Источник и Назначение укажите созданную VPN-зону и внутренние зоны, к которым необходимо обеспечить доступ с удаленных площадок.
5. Нажмите Сохранить.