Table of Contents

Table of Contents 1
Настройка VPN (версия 7.5.0 и выше) 2
- Общие принципы 3
- Настройка VPN для защищенного соединения офисов 4
- Настройка VPN для удаленного доступа в сеть 8
- Журналирование событий VPN-сервера 11
- VPN в режиме полного туннелирования 15
- Раздельное туннелирование для UserGate Client 16
- Особенности конвертации правил VPN при обновлении до версии 7.5.x 18
- Управление VPN-сессиями 20
- Примеры настройки 22
  - Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1) 23
  - Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1) с помощью интерфейса CLI 30
  - Пример настройки site-to-site VPN с IPSec (IKEv2) и аутентификацией посредством сертификатов 34
  - Пример настройки удаленного доступа в сеть для конечного устройства на Astra Linux 40

Настройка VPN (версия 7.5.0 и выше)

Общие принципы

Product: NGFW
Technology: VPN
Version: 7.x, 7.5.x

С помощью функции VPN-сервера на UserGate NGFW вы можете создавать VPN-подключения следующих типов:

- Защищенное соединение офисов (site-to-site VPN). Подключение типа сервер-сервер позволяет объединить офисы компании в единую логическую сеть. UserGate NGFW может выступать как в роли узла-инициатора соединения (initiator), так и в роли узла-ответчика (responder).
- Удаленный доступ клиентов в сеть офиса (remote access VPN). В этом сценарии UserGate NGFW выступает в роли VPN-сервера, а устройства пользователей с установленным VPN-клиентом — в роли конечных устройств. В качестве VPN-клиента на устройствах пользователей может использоваться ПО UserGate Client (клиенты для Windows, Linux и macOS), также поддерживаются встроенные VPN-клиенты большинства известных операционных систем, таких как Windows, Linux, Mac OS X, iOS, Android.

Серверные правила VPN в UserGate NGFW версии 7.5.0 и выше реализованы в виде модульной структуры, состоящей из трех отдельно настраиваемых объектов:

- правил подключения;
- правил аутентификации;
- политик VPN.

С помощью такого подхода обеспечивается гибкость в комбинировании параметров на каждом этапе — от инициации сессии до применения индивидуальных настроек доступа в сеть для отдельных пользователей или групп пользователей. Одному методу подключения может соответствовать несколько способов аутентификации; каждому способу аутентификации может соответствовать один или несколько вариантов сетевых параметров подключения.

Подробнее о настройке VPN-подключений типа site-to-site — в разделе « Настройка VPN для защищенного соединения офисов », о настройке VPN-подключений типа remote access — в разделе « Настройка VPN для удаленного доступа в сеть».

Настройка VPN для защищенного соединения офисов

Technology: VPN
Version: 7.x, 7.5.x
Product: NGFW

Примечание В этом разделе описан алгоритм настройки параметров VPN-соединений для версии 7.5.0 и выше.

VPN-подключение, с помощью которого создается защищенное соединение локальных сетей удаленных офисов, называется site-to-site VPN.

При подключении один VPN-сервер выступает в роли инициатора соединения (initiator), а другой — в роли ответчика (responder). После успешного создания туннеля распределение ролей VPN-серверов не оказывает влияния на характеристики соединения — передача данных через туннель осуществляется двунаправленно и симметрично.

Вы можете создать VPN-подключение между устройствами UserGate NGFW, либо между UserGate NGFW и VPN-шлюзами сторонних производителей. UserGate NGFW может выступать как в роли инициатора соединения, так и в роли ответчика.

При создании VPN-туннелей в сценарии site-to-site могут использоваться протоколы:

- L2TP/IPsec (IKEv1) — только между устройствами UserGate;
- IPsec (IKEv1);
- IPsec (IKEv2).

Для создания VPN-подключения необходимо выполнить настройки соответствующих параметров на обоих граничных узлах защищенного соединения: узле-инициаторе и узле-ответчике.

Настройка UserGate NGFW в качестве узла-ответчика

Для работы UserGate NGFW в качестве VPN-сервера (ответчика) в сценарии site-to-site VPN необходимо настроить:

- сетевые параметры;
- параметры аутентификации;
- правила подключения;
- правила аутентификации;
- политики VPN;
- доступ к сетевым ресурсам.

Настройка сетевых параметров

На узле UserGate NGFW, исполняющем роль VPN-сервера (ответчика), необходимо выполнить ряд дополнительных настроек сетевых параметров:

- разрешить доступ к узлу для установления VPN-соединения;
- создать зону для контроля подключаемых узлов;
- создать VPN-интерфейс для организации туннеля.

Предоставление доступа для VPN-соединений

В настройках зоны, из которой будут подключаться узлы-инициаторы (например, Untrusted), активируйте доступ к сервису VPN. Для этого в веб-консоли UserGate NGFW перейдите в раздел **Настройки → Сеть → Зоны**, затем в параметрах контроля доступа зоны поставьте флажок для сервиса VPN. Подробнее о создании и настройках параметров зон — в разделе «Настройка зон».

Создание зоны для VPN-подключений

Создайте зону, к которой будут принадлежать подключаемые по VPN узлы. Эту зону в дальнейшем можно будет использовать в правилах политик безопасности.

В веб-консоли UserGate NGFW зоны создаются в разделе **Настройки → Сеть → Зоны**. Подробнее о создании и настройках зон — в разделе « Настройка зон».

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения узлов-инициаторов VPN-подключения. Такой тип интерфейса является кластерным — он будет автоматически создаваться на всех узлах UserGate NGFW, входящих в кластер конфигурации. Если настроен кластер отказоустойчивости, узлы-инициаторы будут автоматически переключаться на резервный узел VPN-сервера в случае обнаружения проблем с активным узлом.

В веб-консоли UserGate NGFW VPN-интерфейс создается в разделе **Настройки → Сеть → Интерфейсы**. Для создания интерфейса нажмите **Добавить** и выберите **Добавить VPN**. Подробнее о создании VPN-интерфейса — в разделе «Настройка интерфейсов».

Настройка параметров аутентификации

Порядок взаимной аутентификации узлов, участвующих в организации site-to-site VPN, описывается правилами аутентификации.

Чтобы настроить правила аутентификации, сначала необходимо создать набор средств аутентификации (например, общие ключи, сертификаты или профили клиентских сертификатов), которые затем будут использоваться в правилах в зависимости от выбранного метода аутентификации.

При настройке защищенного IPsec-соединения могут понадобиться следующие средства аутентификации узлов:

- Общий ключ (pre-shared key, PSK). Используется для аутентификации в протоколах IKEv1 и IKEv2. Ключ задается в параметрах правил подключения (для IKEv1) или правил аутентификации (для IKEv2) на VPN-сервере (ответчике), а также в настройках параметров подключения на узле-инициаторе. Для успешного установления соединения значения ключа на обеих сторонах должны совпадать.
- Сертификаты VPN-серверов. Применяются для аутентификации с использованием инфраструктуры открытых ключей (PKI) в протоколе IKEv2. Такие сертификаты необходимо заранее создать и импортировать в UserGate NGFW.

  О примерах создания и использования сертификатов для IKEv2 VPN — в разделе « Приложение». О правилах импорта сертификатов в UserGate NGFW — в разделе « Управление сертификатами».
- Профили клиентских сертификатов. Позволяют идентифицировать узел-инициатор по определенному атрибуту его сертификата, а также проверить цепочку доверия и подлинность сертификата с учетом списков отозванных сертификатов. При создании профиля используются сертификаты корневых и промежуточных удостоверяющих центров, выдавших сертификаты узлов-инициаторов. Подробнее о профилях клиентских сертификатов — в разделе «Профили клиентских сертификатов».

  Чтобы VPN-сервер мог проверить IP-адрес узла-инициатора при установлении соединения по IPsec IKEv2, в сертификате инициатора в поле iPAddress расширения SAN (Subject Alternative Name) должен быть указан тот IP-адрес, с которого поступит запрос на подключение. При этом в профиле клиентского сертификата на VPN-сервере в параметре **Получать имя пользователя из** необходимо выбрать значение **Subject altname IPv4**.

  Если между узлом-инициатором и VPN-сервером используется NAT, IP-адрес из сертификата не совпадет с фактическим адресом источника пакетов, из-за чего соединение не будет установлено. Для такого сценария можно в поле **Получать имя пользователя из** в профиле клиентского сертификата выбрать любое другое значение, кроме **Subject altname IPv4**, VPN-сервер в таком случае не будет выполнять проверку IP-адреса инициатора соединения.

Для настройки VPN-туннеля с использованием протокола L2TP на стороне VPN-сервера (ответчика) необходимо создать учетную запись для аутентификации узла-инициатора, а также настроить профиль аутентификации, определяющий применяемый метод проверки подлинности.

В веб-консоли UserGate NGFW профили аутентификации создаются в разделе **Настройки → Пользователи и устройства → Профили аутентификации**. Подробнее о профилях аутентификации — в разделе « Профили аутентификации».

Настройка правил подключения

Правила подключения описывают первый этап установления соединения. Он начинается с инициирования соединения VPN-клиентом (узлом-инициатором) и завершается ответом VPN-сервера (узла-ответчика) — предложением выполнить обмен ключами либо отказом с разрывом соединения. В правилах задаются проверки зоны источника, адреса инициатора и назначения, типа протокола, а также определяются параметры первой фазы установления защищенного соединения.

Для создания правила подключения в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила подключения** и нажмите **Добавить**.
2. Выберите протокол подключения **IKE**.
3. На вкладке **Общие** в свойствах протокола IKE:

- Укажите название и описание правила;
- Выберите версию протокола IKE:
    - **IKEv1PSK**. Для этого протокола выберите режим работы IKEv1 (основной или агрессивный) и укажите значение общего ключа (pre-shared key). Ключ должен совпадать на узле-инициаторе и на узле-ответчике.
    - **IKEv2**.

4. На вкладке **Источник** укажите зоны и адреса, с которых разрешено принимать подключения к VPN:

- Укажите зону инициатора подключения;
- Укажите адрес инициатора подключения:
    - выберите или создайте список IP-адресов;
    - выберите или создайте список доменов;
    - выберите GeoIP.

ПримечаниеОбработка трафика происходит по следующей логике:

- условия объединяются по логическому ИЛИ, если указаны несколько списков IP-адресов или доменов;
- условия объединяются по логическому И, если указаны GeoIP и списки IP-адресов или доменов.

5. На вкладке **Назначение** выберите или создайте список IP-адресов или доменных имен интерфейса, на который будут приходить запросы на VPN-подключение. Интерфейс должен принадлежать зоне, указанной на этапе контроля доступа зоны.

6. На вкладке **Фаза 1** укажите параметры настройки фазы 1 для установления защищенного канала IKE SA:

- Укажите время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1.
- Укажите параметры работы механизма Dead Peer Detection (DPD) для проверки работоспособности канала и его своевременного отключения или переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны три режима работы механизма:
    - **Отключено** — механизм отключен. DPD-запросы не отсылаются.
    - **Всегда включено** — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов. Если ответ не пришел, соединение завершается.
    - **При отсутствии трафика** — DPD-запросы не отсылаются, пока есть ESP-трафик через созданный канал. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.
- Выберите группы Диффи-Хеллмана, которые будут использоваться для обмена ключами.
- Выберите алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.

О создании правил подключения с помощью команд интерфейса командной строки — в разделе « Настройка серверных правил».

Настройка правил аутентификации

Правила аутентификации описывают второй этап установления соединения. Он начинается с ответа узла-инициатора на предложение обмена ключами и завершается после успешной аутентификации. В этих правилах задаются проверки типа аутентификации и определяются параметры второй фазы установления защищенного соединения.

Для создания правила аутентификации в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила аутентификации** и нажмите **Добавить**.
2. Выберите сценарий **site-to-site** и затем протокол установления защищенного соединения:
    - **IPsec only**/**IKEv1**;
    - **IKEv2**;
    - **IPsec**/**L2TP**.
3. На вкладке **Общие** в свойствах выбранного протокола:
    - Для протокола IPsec only/IKEv1:
        - Укажите название и описание правила;
        - Выберите одно или несколько созданных ранее правил подключения.
    - Для протокола IKEv2:
        - Укажите название и описание правила;
        - Выберите режим аутентификации (PKI или PSK):
            - Для аутентификации с помощью сертификатов (PKI) укажите созданные ранее сертификат сервера и профиль клиентского сертификата;
            - Для аутентификации с помощью общего ключа (PSK) укажите общий ключ и созданный ранее сертификат сервера.
        - Укажите параметры взаимной идентификации граничных узлов соединения: инициатора (initiator) и ответчика (responder). В качестве идентификатора можно указать IP-адрес узла или FQDN.
        - Выберите одно или несколько созданных ранее правил подключения.
    - Для протокола IPsec/L2TP:
        - Укажите название и описание правила;
        - Выберите созданный ранее профиль аутентификации для пользователей VPN.
        - Укажите параметры взаимной идентификации граничных узлов соединения: инициатора (initiator) и ответчика (responder). В качестве идентификатора можно указать IP-адрес узла или FQDN.
        - Выберите одно или несколько созданных ранее правил подключения.
4. На вкладке **Фаза 2** укажите параметры настройки фазы 2 для установления защищенного канала IPsec SA:
    - Укажите время жизни ключа. По истечении этого времени узлы должны сменить ключ шифрования.
    - Укажите максимальный размер данных, шифруемых одним ключом.

ПримечаниеЕсли заданы оба параметра (время жизни ключа и максимальный размер данных, шифруемых одним ключом), то первый достигнувший предела параметр запустит пересоздание ключей сессии.

- При необходимости включите параметр NAT keepalive. NAT keepalive применяется в сценариях, когда IPsec-трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN-туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN-туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону противоположного узла соединения для поддержания сессии NAT активной.
- Выберите алгоритмы аутентификации и шифрования в блоке **Безопасность**. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.
- Для протоколов IPsec only/IKEv1 и IKEv2 в блоке **Peer networks** укажите адреса локальных и удаленных подсетей. Адреса подсетей используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения. Если поставить флажок **Не проверять сети инициатора**, VPN-сервер не будет проверять подсети инициатора соединения в селекторе трафика при организации защищенного канала передачи данных. Функция удобна для подключения множества клиентов (инициаторов) по одному правилу.

  Для протокола IKEv2 можно разрешить работу протоколов динамической маршрутизации через туннель.

О создании правил аутентификации с помощью команд интерфейса командной строки — в разделе « Настройка серверных правил».

Настройка политик VPN

Политики VPN описывают третий этап установления соединения. Он начинается с идентификации узла-инициатора и завершается назначением сетевых параметров подключения: туннельного интерфейса, пула IP-адресов внутри VPN-туннеля, маршрутов к ресурсам через туннель и адресов DNS-серверов.

Для создания политики VPN в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Политики VPN** и нажмите **Добавить**.
2. Выберите сценарий **site-to-site** и затем протокол установления VPN-туннеля:
    - **IPsec**;

- **IPsec/L2TP**.

3. Для протокола IPsec:
   - На вкладке **Общие** в свойствах протокола:
     - Укажите название и описание правила.
     - Выберите VPN-адаптер, который будет использоваться для установления подключения.
     - Выберите одно или несколько созданных ранее правил аутентификации.
4. Для протокола IPsec/L2TP:
   - На вкладке **Общие** в свойствах протокола:
     - Укажите название и описание правила.
     - Выберите одно или несколько созданных ранее правил аутентификации.
   - На вкладке **Пользователи** выберите учетные записи или группы, созданные для серверов, которым разрешено подключаться по VPN.
   - На вкладке **Подсети для VPN**:
     - Укажите VPN-интерфейс, который будет использоваться для подключения.
     - Укажите диапазон IP-адресов, которые будут использованы узлами-инициаторами подключения. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу UserGate NGFW, используемому совместно с этой сетью. Не указывайте адреса сети и широковещательный адрес.
     - Укажите маску сети VPN.
     - Укажите DNS-серверы, которые будут переданы узлу-инициатору подключения, или поставьте флажок **Использовать системные DNS**, в этом случае узел-инициатор будет использовать системные DNS-серверы.
   - На вкладке **Маршруты VPN** укажите маршруты, передаваемые узлу-инициатору в виде бесклассовой адресации (CIDR) или заранее созданный список IP-адресов.

О создании политик VPN с помощью команд интерфейса командной строки — в разделе « Настройка серверных правил».

Настройка доступа к ресурсам

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в веб-консоли UserGate NGFW в разделе **Настройки → Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из зоны для VPN-подключений в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана — в разделе « Межсетевой экран».

Для примера в веб-консоли создано правило межсетевого экрана VPN for site-to-site to Trusted and Untrusted, разрешающее весь трафик из зоны VPN for site-to-site в зоны Trusted и Untrusted. Правило отключено по умолчанию

Чтобы трафик передавался обратно клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например созданную ранее зону для VPN-подключений.

Настройка UserGate NGFW в качестве узла-инициатора подключения

Для работы UserGate NGFW в качестве инициатора VPN-соединения в сценарии site-to-site VPN необходимо настроить:

- сетевые параметры;
- параметры аутентификации;
- параметры подключения клиента;
- клиентские правила.

Настройка сетевых параметров

На узле UserGate NGFW, исполняющем роль инициатора VPN-соединения, необходимо выполнить ряд дополнительных настроек сетевых параметров:

- создать зону для контроля VPN-подключений;
- создать VPN-интерфейс для организации туннеля.

Создание зоны для VPN-подключений

Создайте зону, которой будут принадлежать интерфейсы, используемые для подключения по VPN. В веб-консоли UserGate NGFW зоны создаются в разделе **Настройки → Сеть → Зоны** . Подробнее о создании и настройках зон — в статье «Настройка зон».

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения по VPN.

В веб-консоли UserGate NGFW VPN-интерфейс создается в разделе **Настройки → Сеть → Интерфейсы** . Для создания интерфейса нажмите **Добавить** и выберите **Добавить VPN**, далее в настройках VPN-адаптера задайте необходимые параметры. Подробнее о создании VPN-интерфейса — в разделе «Настройка интерфейсов».

Контроль доступа к сетевым ресурсам

Чтобы трафик передавался на VPN-сервер из нужной зоны узла-источника через VPN-туннель, создайте правило межсетевого экрана, разрешающее трафик между зоной для VPN-подключений и зонами назначения . Подробнее о создании и настройке правил межсетевого экрана — в разделе «Межсетевой экран».

Настройка параметров аутентификации

При настройке защищенного IPsec-соединения с использованием протокола IKEv2 можно применять аутентификацию на основе сертификатов (PKI). Для этого необходимо заранее создать сертификат и импортировать его на узел, выступающий в роли VPN-клиента (инициатора соединения), через веб-интерфейс в разделе **Настройки → Консоль администратора → Сертификаты** ..

ПримечаниеЕсли VPN-сервер выполняет проверку IP-адреса узла-инициатора соединения по сертификату, сертификат узла-инициатора должен содержать значение IP-адреса, с которого придет запрос на подключение к VPN-серверу, в поле iPAddress расширения SAN (Subject Alternative Name).

О примерах создания и использования сертификатов для IKEv2 VPN — в разделе « Приложение».

Настройка параметров подключения

При настройке VPN-подключения указываются используемые протоколы для установления соединения, выбираются методы аутентификации, а также определяются параметры обеих фаз формирования защищенного канала.

Для настройки параметров подключения узла-инициатора в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN site-to-site клиент → Подключение клиента** и нажмите **Добавить**.
2. Выберите протокол установления защищенного соединения:
   - **IPsec only/IKEv1**;
   - **IKEv2**;
   - **IPsec/L2TP**.
3. На вкладке **Общие** в свойствах выбранного протокола:
   - Для протокола IPsec only/IKEv1:
     - Укажите название и описание подключения;
     - Выберите режим работы IKE (основной или агрессивный);
     - Укажите общий ключ (pre-shared key). Ключ должен совпадать на узле-инициаторе и на узле-ответчике.
     - Укажите параметр идентификации узла-инициатора. В качестве идентификатора можно указать IP-адрес узла или FQDN.

       Если флажок не поставлен, механизм согласования сетевых параметров для проверки IP-адреса туннельного интерфейса на VPN-сервере не применяется. Значение IP-адреса определяется настройками туннельного интерфейса на узле-инициаторе.
   - Для протокола IKEv2:
     - Укажите название и описание подключения;
     - Флажок **Проверять IP на VPN-сервере** определяет, будет ли узел-инициатор соединения запрашивать проверку IP-адреса у VPN-сервера (параметр необходим только для установки соединений с

узлами-ответчиками версий ниже 7.5.0). VPN-сервер может принять предложенный IP-адрес или назначить другой. Если флажок поставлен, узел-инициатор соединения добавляет параметр Payload Configuration в сообщение IKE_AUTH и передает в поле INTERNAL_IP4_ADDRESS значение, зависящее от типа туннельного интерфейса:

- Для туннельного интерфейса с динамическим назначением IP-адреса в поле INTERNAL_IP4_ADDRESS передается значение 0.0.0.0/0, что является запросом на динамическое выделение IP-адреса. VPN-сервер, получив значение 0.0.0.0/0, выделяет IP-адрес из собственного пула, заданного в параметрах соединения на сервере.
- Для туннельного интерфейса со статическим IP-адресом в поле INTERNAL_IP4_ADDRESS передается его IP-адрес. VPN-сервер использует это значение для проверки соответствия политике подключения.

- Выберите режим аутентификации (PKI или PSK):
  - Для аутентификации с помощью сертификатов (PKI) укажите сертификат узла-инициатора;
  - Для аутентификации с общим ключом (PSK) укажите общий ключ. Ключ должен совпадать на узле-инициаторе и на узле-ответчике.
- Укажите параметр идентификации узла-инициатора. В качестве идентификатора можно указать IP-адрес узла или FQDN.

- Для протокола IPsec/L2TP:
  - Укажите название и описание подключения;
  - Выберите режим работы IKE (основной или агрессивный);
  - Укажите общий ключ (pre-shared key). Ключ должен совпадать на узле-инициаторе и на узле-ответчике.
  - Укажите параметры взаимной идентификации граничных узлов соединения: инициатора (**Initiator**) и ответчика (**Responder**). В качестве идентификатора можно указать IP-адрес узла или FQDN.
  - Укажите параметры аутентификации (логин и пароль) узла-инициатора на узле-ответчике. Параметры аутентификации должны соответствовать параметрам учетной записи, созданной при настройке узла-ответчика.

4. На вкладке **Фаза 1** укажите параметры настройки фазы 1 для установления защищенного канала IKE SA:
   - Укажите время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1.
   - Укажите параметры работы механизма Dead Peer Detection (DPD) для проверки работоспособности канала и его своевременного отключения или переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны три режима работы механизма:
     - **Отключено** — механизм отключен. DPD-запросы не отсылаются.
     - **Всегда включено** — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается.
     - **При отсутствии трафика** — DPD-запросы не отсылаются, пока есть ESP-трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.
   - Выберите группы Диффи-Хеллмана, которые будут использоваться для обмена ключами.
   - Выберите алгоритмы аутентификации и шифрования в блоке **Безопасность**. Алгоритмы, используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.
5. На вкладке **Фаза 2** укажите параметры настройки фазы 2 для установления защищенного канала IPsec SA:
   - Укажите время жизни ключа. По истечении этого времени узлы должны сменить ключ шифрования.
   - Укажите максимальный размер данных, шифруемых одним ключом.

   ПримечаниеЕсли заданы оба значения (время жизни ключа и максимальный размер данных, шифруемых одним ключом), то первый достигнувший предела параметр запустит пересоздание ключей сессии.
   - Выберите алгоритмы аутентификации и шифрования в блоке **Безопасность**. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.
   - Для протоколов IPsec only/IKEv1 и IKEv2 в блоке **Peer networks** укажите адреса локальных и удаленных подсетей. Адреса подсетей используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения.

     Для протокола IKEv2 можно разрешить работу протоколов динамической маршрутизации через туннель.

О настройках параметров подключения узла-инициатора с помощью команд интерфейса командной строки — в разделе «Настройка клиентских правил».

Настройка клиентских правил

Клиентское правило в сценарии site-to-site VPN используется для инициирования подключения к VPN-серверу (узлу-ответчику).

Для настройки клиентского правила в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN site-to-site клиент → Клиентские правила** и нажмите **Добавить**.
2. Укажите название и описание клиентского правила.
3. Выберите одно из созданных ранее подключений клиента.
4. Выберите ранее созданный VPN-интерфейс.
5. Укажите адрес VPN-сервера (ответчика) в формате IP-адреса или FQDN.

О настройках клиентских правил с помощью команд интерфейса командной строки — в разделе «Настройка клиентских правил».

После завершения настройки параметров VPN-сервиса узел-инициатор получает возможность установить соединение с VPN-сервером (ответчиком). При корректной конфигурации параметров будет сформирован VPN-туннель. Для разрыва соединения необходимо отключить клиентское VPN-правило.

Если VPN-соединение не установилось, в разделе клиентского правила в поле **Последняя ошибка** отобразится описание ошибки установления соединения.

События работы VPN-сервера (изменения параметров правил, установление соединений, ошибки установления соединений) записываются в системном журнале событий (Event log). Подробнее — в разделе «Журналирование событий VPN-сервера».

Настройка VPN для удаленного доступа в сеть

Technology: VPN
Version: 7.x, 7.5.x
Product: NGFW
Примечание В этом разделе описан алгоритм настройки параметров VPN-соединений для версии 7.5.0 и выше.

VPN-подключение, с помощью которого пользователи могут получить защищенный доступ к сети компании через интернет, называется remote access VPN.

В этом типе подключения UserGate NGFW выступает в роли VPN-сервера, а устройства пользователей — в роли конечных устройств. В качестве клиентского ПО на устройствах пользователей может использоваться UserGate Client, также поддерживаются встроенные клиенты большинства известных операционных систем, таких как Windows, Linux, macOS, iOS, Android.

Для организации защищенного соединения могут использоваться протоколы:

- IPsec (IKEv2);
- DTLS — только при работе с UserGate Client;
- L2TP/IPsec (IKEv1) — только для работы со встроенными VPN-клиентами операционных систем.

Для создания VPN-подключения необходимо произвести настройку соответствующих параметров на VPN-сервере, а затем настроить и подключить VPN-клиент на конечном устройстве.

Настройка VPN-сервера на UserGate NGFW

Для работы UserGate NGFW в качестве VPN-сервера в сценарии remote access VPN необходимо настроить:

- сетевые параметры;
- параметры аутентификации;
- правила подключения;
- правила аутентификации;
- политики VPN;
- доступ к сетевым ресурсам.

Настройка сетевых параметров

На узле UserGate NGFW необходимо выполнить ряд дополнительных настроек сетевых параметров:

- разрешить доступ к узлу для установления VPN-соединения;
- создать зону для контроля подключаемых конечных устройств;
- создать VPN-интерфейс для организации туннеля.

Предоставление доступа для VPN-соединений

Откройте доступ к сервису VPN в свойствах зоны, из которой будут подключаться конечные устройства.

В параметрах зоны, из которой будут подключаться конечные устройства (например, Untrusted), активируйте доступ к сервису VPN. Для этого в веб-консоли UserGate NGFW перейдите в раздел **Настройки → Сеть → Зоны** , затем в параметрах контроля доступа зоны поставьте флажок для сервиса VPN. Подробнее о создании и настройках параметров зон — в разделе «Настройка зон».

Создание зоны для VPN-подключений

Создайте зону, которой будут принадлежать подключаемые по VPN конечные устройства. Эту зону в дальнейшем можно будет использовать в правилах политик безопасности.

В веб-консоли UserGate NGFW зоны создаются в разделе **Настройки → Сеть → Зоны** . Подробнее о создании и настройках зон — в разделе « Настройка зон».

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения конечных устройств. Такой тип интерфейса является кластерным — он будет автоматически создаваться на всех узлах UserGate NGFW, входящих в кластер конфигурации. Если настроен кластер отказоустойчивости, конечные устройства будут автоматически переключаться на резервный узел в случае обнаружения проблем с активным узлом.

В веб-консоли UserGate NGFW VPN-интерфейс создается в разделе **Настройки → Сеть → Интерфейсы** . Для создания интерфейса нажмите **Добавить** и выберите **Добавить VPN**. Подробнее о создании VPN-интерфейса — в разделе «Настройка интерфейсов».

Настройка параметров аутентификации

Порядок аутентификации в сценарии remote access VPN описывается правилами аутентификации.

Чтобы настроить правила аутентификации, сначала необходимо создать набор средств аутентификации (например, общие ключи, сертификаты или профили клиентских сертификатов), которые затем будут использоваться в правилах в зависимости от выбранного метода аутентификации.

При настройке защищенного IPsec-соединения могут понадобиться следующие средства аутентификации узлов:

- Общий ключ (pre-shared key, PSK). Применяется при использовании протокола IKEv1 для организации защищенного соединения со встроенными VPN-клиентами операционных систем. Общий ключ задается в параметрах правил подключения на VPN-сервере и в настройках VPN-клиента на устройстве пользователя. Для успешного установления соединения значения ключа на обеих сторонах должны совпадать.
- Сертификат. Используется при выборе протоколов IKEv2 или DTLS для организации защищенного соединения. В этом случае необходимо заранее создать сертификаты для VPN-сервера и конечных устройств, а затем импортировать их в UserGate NGFW и на конечные устройства. Подробнее о правилах импорта сертификатов в UserGate NGFW — в разделе «Управление сертификатами».
- Профили клиентских сертификатов. Позволяют идентифицировать конечное устройство по определенному атрибуту его сертификата, а также проверить цепочку доверия и подлинность сертификата с учетом списков отозванных сертификатов. При создании профиля используются сертификаты корневых и промежуточных удостоверяющих центров, участвовавших в выдаче сертификатов конечным устройствам. Подробнее о профилях клиентских сертификатов — в разделе «Профили клиентских сертификатов».

Для аутентификации VPN-пользователей необходимо создать соответствующий профиль аутентификации. Он настраивается в разделе **Настройки → Пользователи и устройства → Профили аутентификации** . Допускается использование того же профиля, который применяется для аутентификации пользователей при доступе в интернет. При этом следует учитывать, что для VPN-аутентификации не поддерживаются методы прозрачной аутентификации, такие как Kerberos, NTLM и SAML IDP. Подробнее о профилях аутентификации — в разделе «Профили аутентификации».

ПримечаниеЕсли авторизация пользователей происходит в различных поддоменах, на вкладке «Домены LDAP» в настройках LDAP-коннектора необходимо указывать все варианты таких поддоменов. Подробнее о настройке LDAP-коннектора читайте в разделе «Серверы аутентификации».

Для аутентификации пользователей VPN вы также можете использовать метод многофакторной аутентификации. Значение второго фактора аутентификации может быть получено через одноразовые коды TOTP. VPN с TOTP работает для клиента UserGate Client с протоколами IKEv2 или DTLS (код вводится в отдельном окне), для других клиентов — только с протоколом IKEv1 (код вводится в пароле через двоеточие: пароль_пользователя:totp_code).

ПримечаниеПри установлении L2TP\IPsec VPN-соединения с аутентификацией пользователей через Multifactor RADIUS Adapter повторное переподключение к VPN-серверу в течении 30-секундного тайм-аута с момента предыдущего успешного подключения произойдет без обращением к RADIUS-серверу. Если переподключение будет выполняться за пределами 30-секундного тайм-аута, обращение к RADIUS-серверу произойдет.

Настройка правил подключения

Правила подключения описывают первый этап установления соединения. Он начинается с инициирования соединения VPN-клиентом и завершается ответом VPN-сервера — предложением выполнить обмен ключами либо отказом с разрывом соединения. В правилах задаются проверки зоны источника, адреса инициатора и назначения, типа протокола, а также определяются параметры первой фазы установления защищенного соединения.

Для создания правила подключения в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила подключения** и нажмите **Добавить**.
2. Выберите протокол подключения (**IKE** или **DTLS**).

   ПримечаниеДля работы DTLS на интерфейсе должен быть настроен только один IP-адрес. Использование интерфейсов с дополнительными (secondary) IP-адресами не поддерживается.

   В кластере DTLS можно использовать при условии, что на интерфейсе настроен только виртуальный IP-адрес (VIP), без дополнительных IP-адресов.
3. На вкладке **Общие** в свойствах выбранного протокола укажите:
   - Для протокола IKE:

- Укажите название и описание правила;
- Выберите версию протокола IKE:
  - **IKEv1PSK**. Укажите режим работы IKEv1 (основной или агрессивный) и значение общего ключа (pre-shared key). Ключ должен совпадать на VPN-сервере и на VPN-клиенте;
  - **IKEv2**.
- Для протокола DTLS укажите название и описание правила.

4. На вкладке **Источник** укажите зоны и адреса, с которых разрешено принимать подключения к VPN:
   - Укажите зону инициатора подключения;
   - Укажите адрес инициатора подключения:
     - выберите или создайте список IP-адресов;
     - выберите или создайте список доменов;
     - выберите GeoIP.

ПримечаниеОбработка трафика происходит по следующей логике:

- условия объединяются по логическому ИЛИ, если указаны несколько списков IP-адресов или доменов;
- условия объединяются по логическому И, если указаны GeoIP и списки IP-адресов или доменов.

5. На вкладке **Назначение** выберите или создайте список IP-адресов или доменных имен интерфейса, на который будут приходить запросы на VPN-подключения от конечных устройств. Интерфейс должен принадлежать зоне, указанной на этапе контроля доступа зоны.

6. На вкладке **Фаза 1** укажите криптографические параметры фазы 1 согласования защищенного соединения:
   - Укажите время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1.
   - Укажите параметры работы механизма Dead Peer Detection (DPD) для проверки работоспособности канала и его своевременного отключения или переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны три режима работы механизма:
     - **Отключено** — механизм отключен. DPD-запросы не отсылаются.
     - **Всегда включено** — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD-запросов. Если ответ не пришел, соединение завершается.
     - **При отсутствии трафика** — DPD-запросы не отсылаются, пока есть ESP-трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.
   - В разделе **Безопасность** выберите алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.
   - Для протокола IKE выберите группы Диффи-Хеллмана, которые будут использоваться для обмена ключами.

О создании правил подключения с помощью команд интерфейса командной строки — в разделе « Настройка серверных правил».

Настройка правил аутентификации

Правила аутентификации описывают второй этап установления соединения. Он начинается с ответа VPN-клиента на предложение обмена ключами и завершается после успешной аутентификации. В этих правилах задаются проверки типа аутентификации и определяются параметры второй фазы установления защищенного соединения.

Для создания правила аутентификации в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила аутентификации** и нажмите **Добавить**.
2. Выберите сценарий **Удаленный доступ** и затем протокол установления защищенного соединения:
   - **IPsec/L2TP;**
   - **IKEv2**;
   - **DTLS**.
3. На вкладке **Общие** в свойствах выбранного протокола укажите:
   - Для протокола IPsec/L2TP:
     - Укажите название и описание правила;
     - Выберите созданный ранее профиль аутентификации;
     - Выберите одно или несколько созданных ранее правил подключения.
   - Для протоколов IKEv2 и DTLS:
     - Укажите название и описание правила;
     - Укажите импортированный ранее сертификат сервера и созданный ранее профиль аутентификации;
     - Выберите режим аутентификации (AAA, PKI или любой):
       - Для аутентификации с помощью ключей (PKI) укажите профиль клиентских сертификатов.
       - В режиме аутентификации с помощью методов EAP, PEAP (AAA) VPN-клиент обменивается с VPN-сервером EAP-пакетами. VPN-сервер транслирует пакеты на внешний доменный RADIUS-сервер, который принимает решение об авторизации. После получения разрешения от RADIUS-сервера, VPN-сервер по полученному логину запрашивает у сервера домена информацию о пользователе, после чего принимает решение о подключении пользователя к VPN.
     - Выберите одно или несколько созданных ранее правил подключения.
4. На вкладке **Фаза 2** укажите криптографические параметры фазы 2 согласования защищенного соединения:
   - Укажите максимальный размер данных, шифруемых одним ключом.
   - При необходимости включите параметр NAT keepalive. NAT keepalive применяется в сценариях, когда IPsec-трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN-туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN-туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону VPN-клиента для поддержания сессии NAT активной.
   - Дополнительно для протоколов IKEv2 и IKEv1/L2TP:
     - Укажите время жизни ключа. По истечению этого времени узлы должны сменить ключ шифрования.

ПримечаниеЕсли заданы значения обоих параметров (время жизни ключа и максимальный размер данных, шифруемых одним ключом), то первый достигнувший предела счетчик запустит пересоздание ключей сессии.

   - Выберите алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.

О создании правил аутентификации с помощью команд интерфейса командной строки — в разделе « Настройка серверных правил».

Настройка политик VPN

Политики VPN описывают третий этап установления соединения. Он начинается с идентификации VPN-клиента и завершается назначением сетевых параметров подключения: туннельного интерфейса, пула IP-адресов внутри VPN-туннеля, маршрутов к ресурсам через туннель и адресов DNS-серверов.

Для создания политики VPN в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Политики VPN** и нажмите **Добавить**.
2. Выберите сценарий **Удаленный доступ** и затем тип VPN-клиента:
   - **Clients** — для встроенных VPN-клиентов известных операционных систем;
   - **UserGate Client** — для VPN-клиента UserGate Client.
3. На вкладке **Общие** в свойствах удаленного доступа:
   - Укажите название и описание правила;
   - Выберите одно или несколько созданных ранее правил аутентификации.
4. На вкладке **Пользователи** выберите локальную или доменную учетную запись или группу, которые будут использоваться для аутентификации пользователей.
5. На вкладке **Подсети для VPN**:

- Укажите VPN-интерфейс, который будет использоваться для подключения.
- Укажите диапазон IP-адресов, которые будут использованы для подключения. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу UserGate NGFW, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.
- Укажите маску сети VPN.
- Укажите DNS-серверы, которые будут переданы VPN-клиенту, или поставьте флажок **Использовать системные DNS**, в этом случае клиенту будут назначены локальные DNS-серверы, которые использует UserGate NGFW.

6. Для встроенных VPN-клиентов операционных систем на вкладке **Маршруты VPN** укажите маршруты, передаваемые конечному устройству в виде бесклассовой адресации (CIDR) или заранее созданного списка IP-адресов.

7. Для UserGate Client укажите параметры настройки функции раздельного туннелирования (split tunneling). Подробнее — в разделе « Настройка раздельного туннелирования для UserGate Client ».

О создании политик VPN с помощью команд интерфейса командной строки — в разделе « Настройка серверных правил».

Настройка доступа к ресурсам

Клиенты подключаются к VPN с использованием протокола Point-to-Point. Чтобы трафик мог ходить из созданной ранее зоны для VPN-подключений, создайте правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Настройки → Политики сети → NAT и маршрутизация** . Подробнее о правилах NAT — в разделе « NAT и маршрутизация». Для примера в веб-консоли UserGate NGFW создано правило NAT from VPN for remote access to Trusted and Untrusted, разрешающее подмену IP-адресов из зоны VPN for remote access в зоны Trusted и Untrusted.

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в веб-консоли UserGate NGFW в разделе **Настройки → Политики сети → Межсетевой экран** создайте правило межсетевого экрана, разрешающее трафик из зоны для VPN-подключений в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана — в разделе «Межсетевой экран».

Для примера в веб-консоли UserGate NGFW создано правило межсетевого экрана VPN for remote access to Trusted and Untrusted, разрешающее весь трафик из зоны VPN for remote access в зоны Trusted и Untrusted. Правило отключено по умолчанию.

Настройка параметров VPN-клиента

После настройки правил VPN-сервера необходимо настроить параметры подключения VPN-клиентов. В качестве клиентского ПО на устройствах пользователей может использоваться UserGate Client, также поддерживаются встроенные клиенты большинства известных операционных систем.

Настройка параметров VPN-клиента зависит от типа клиента и протокола установления VPN-подключения.

Настройка параметров VPN-подключения UserGate Client

О настройках VPN-подключений с помощью UserGate Client для Windows — в разделе « Установка VPN-соединения с помощью UserGate Client для Windows ».

О настройках VPN-подключений с помощью UserGate Client для Linux — в разделе « Настройка VPN-соединения на устройстве пользователя с помощью UserGate Client для Linux ».

О настройках VPN-подключений с помощью UserGate Client для macOS — в разделе « Настройка VPN-соединения на устройстве пользователя с помощью UserGate Client для macOS ».

Настройка параметров VPN-подключения встроенных VPN-клиентов

О настройках VPN-подключений с помощью встроенных VPN-клиентов операционных систем — в разделе « VPN для удаленного доступа клиентов (remote access VPN) ».

Журналирование событий VPN-сервера

Version: 7.x, 7.5.x
Product: NGFW

Записи о работе VPN-сервера UserGate NGFW сохраняются в системном журнале событий (Event log).

Записи содержат информацию:

- об изменениях параметров правил VPN;
- статусе VPN-подключений;
- ошибках VPN-подключений.

В веб-консоли UserGate NGFW в разделе **Журналы и отчеты → Журналы → Журнал событий** записи событий VPN-сервера можно отфильтровать, выбрав в меню журнала компонент «VPN» и нужные типы событий.

Также записи событий можно отфильтровать с помощью запросов в строке расширенного поиска.

ПримечаниеСобытия VPN-сервера не реплицируются на другой узел кластера.

Ошибки подключений на VPN-сервере

Ошибки, связанные с неудачными попытками подключения к VPN-серверу или с разрывом существующих VPN-соединений, записываются в журнал событий UserGate NGFW.

Вы можете отсортировать ошибки подключений в журнале событий по компоненту «VPN», типу события «Ошибка сервера», времени возникновения ошибки, названию клиентского правила или IP-адресу VPN-клиента.

В таблице приведены варианты сообщений об ошибках VPN-подключений, отображаемые в журнале событий веб-интерфейса UserGate NGFW, и возможные причины их возникновения.

Детали события	Event details	Возможная причина ошибки
Клиент не отвечает	No response from client	При согласовании параметров безопасности фазы 1 защищенного соединения не получен ответ от VPN-клиента в установленный промежуток времени. Возможные причины: • Произошла потеря пакетов. • VPN-клиент выключен. • VPN-клиент инициировал новое подключение
Настройки параметров безопасности фазы 1 на сервере несовместимы с настройками на клиенте	The server's Phase 1 security settings are incompatible with the client's settings	На этапе согласования параметров безопасности фазы 1 защищенного соединения не найдены совпадения в параметрах: • групп Диффи-Хеллмана; • алгоритмов шифрования; • алгоритмов аутентификации
Ошибка подключения VPN-клиента: неверный общий ключ	VPN client connection error: incorrect pre-shared key	На этапе установления фазы 1 защищенного соединения VPN-сервер не может расшифровать сообщение от VPN-клиента или подтвердить его подлинность. Возможная причина ошибки: несовпадение значения общего ключа в настройках параметров VPN-сервера и VPN-клиента
Настройки параметров безопасности фазы 2 на сервере несовместимы с настройками на клиенте	The server's Phase 2 security settings are incompatible with the client's settings	На этапе согласования параметров безопасности фазы 2 защищенного соединения не найдены совпадения: • алгоритмов шифрования; • алгоритмов аутентификации
Для клиента не был найден свободный IP-адрес, подключение отклонено	No Available IP Address Found for the Client, Connection Rejected	Диапазон адресов, предназначенный для VPN-клиентов, слишком мал для имеющегося количества одновременных подключений
Не получен код двухфакторной аутентификации	MFA code not received	На этапе аутентификации не получен код второго фактора аутентификации от VPN-клиента
Неверный код двухфакторной аутентификации	MFA verification failed	На этапе аутентификации получен неверный код второго фактора аутентификации от VPN-клиента. Возможные причины получения неверного кода: • Рассинхронизация времени между сервером и клиентом. • Неверно введенный пользователем код. • Устаревший код

Детали события	Event details	Возможная причина ошибки
Цифровая подпись в сертификате клиента не соответствует подписи, вычисленной VPN-сервером	The digital signature in the client certificate does not match the signature computed by the VPN сервер	Ошибка аутентификации на этапе IKE_AUTH в IKEv2. VPN-сервер использует открытый ключ из сертификата клиента для проверки цифровой подписи, которую клиент создал своим закрытым ключом. Если подписи не совпадают, сервер немедленно разрывает соединение, так как не может подтвердить подлинность клиента. Возможные причины: • Несоответствие пары ключей. • Повреждение данных или неправильный расчет хеш-суммы. • Проблемы с цепочкой доверия сертификатов. Сервер не может проверить подпись удостоверяющего центра на клиентском сертификате
В сертификате отсутствует альтернативное имя (SAN) или оно указано неверно	Certificate SAN empty or certificate SAN mismatch	Ошибка при установлении VPN-подключения в сценарии Site-to-Site с аутентификацией посредством сертификатов. Возможной причиной ошибки является некорректный сертификат клиента, в котором либо отсутствует расширение Subject Alternative Name (SAN), либо в нем указан некорректный IP-адрес или FQDN клиента
Несовпадение подсетей клиента и VPN-сервера	Client and server VPN subnets do not match	В сценарии Site-to-site с протоколом IPsec/IKEv2 в ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет ни одного совпадения в адресах локальных и удаленных подсетей, соединение разрывается и выдается сообщение об ошибке
Клиент не поддерживает NAT-T	Client does not support NAT-T	При установлении VPN-подключения с протоколом IPsec IKEv1 VPN-сервер не находит в сообщении от клиента идентификатор Vendor ID
Отсутствует KE-пакет, обмен ключами DH невозможен	Missing KE payload, DH key exchange not possible	Критическая ошибка в процессе обмена ключами при установлении VPN-подключения. Возможные причины: • Ошибки в конфигурации DH-групп на одной из сторон соединения. • Устаревшая версия VPN-клиента. • Блокировки IKE-пакетов на сети
Сбой согласования IKE: не получен nonce (Ni payload) от клиента	IKE negotiation failed: the initiator's nonce was not received	Ошибка в процессе обмена ключами при установлении VPN-подключения. Возможные причины: • Потери пакетов или фрагментация пакетов. • Блокировки IKE-пакетов на сети. • Ошибки конфигурации: разные версии IKE на клиенте и сервере. • Рассинхронизация времени между клиентом и сервером
Сбой аутентификации клиента: хеш-код HASH_I не получен.	Client authentication failed: HASH_I not received	Ошибка аутентификации клиента в процессе установления IKE-соединения. Возможные причины: • Некорректные учетные данные (неправильный общий ключ, недействительный сертификат). • Несовместимость алгоритмов шифрования или аутентификации на клиенте и сервере. • Рассинхронизация времени между клиентом и сервером
Соединение разорвано по алгоритму DPD	VPN connection closed by Dead Peer Detection algorithm	Разрыв VPN-подключения по причине неактивности противоположной стороны соединения в пределах установленного интервала. Причинами отсутствия ответа противоположной стороны соединения могут быть: • Проблемы с сетевой связностью. • Высокая загрузка сети или сторон соединения. • Слишком агрессивные настройки параметров протокола DPD
VPN-туннель закрыт по причине срабатывания защиты от перехвата	VPN tunnel closed due to anti-replay protection trigger	Срабатывание защиты от перехвата и повторной передачи VPN-пакетов. Нарушение последовательности или повторяемость номеров (sequence number) получаемых пакетов. Возможные причины: • Проблемы с сетью (большая потеря пакетов, большая вариация задержек, неправильная очередность доставки пакетов). • Перегрузка VPN-сервера или клиента. • Рассинхронизация времени между клиентом и сервером

Следующие ошибки VPN-подключений не фиксируются в журнале событий UserGate NGFW:

- Несовпадение параметров первого пакета. Если параметры инициирующего пакета от VPN-клиента не соответствуют ни одному из настроенных на VPN-сервере правил подключения.
- Отсутствие активной VPN-политики. Если параметры инициирующего пакета VPN-клиента соответствует условиям одного из правил подключения, но это правило не связано ни с одной из активных политик VPN.
- Промежуточные этапы IKEv2. Отдельные итерации в процессе согласования группы Диффи-Хеллмана по протоколу IKEv2, если в итоге соединение устанавливается успешно.

Ошибки подключений на VPN-сервере (инициаторе соединения)

В сценарии site-to-site VPN UserGate NGFW может выступать в роли инициатора VPN-соединения. При неудачной попытке установления соединения с удаленным VPN-сервером или при разрыве установленного соединения в журнал событий будут записываться сообщения об ошибках VPN-подключения.

В журнале событий веб-интерфейса вы можете отсортировать ошибки подключений по компоненту «VPN», типу события «Ошибка клиента» или времени возникновения ошибки.

Последняя ошибка подключения по активному правилу также отображается в разделе клиентских правил веб-интерфейса (**Настройки → VPN Site-to-Site клиент → Клиентские правила**) в поле **Последняя ошибка VPN**.

В таблице приведены варианты сообщений об ошибках, отображаемые в веб-интерфейсе UserGate NGFW (инициатора соединения), и возможные причины их возникновения.

Детали события	Event details	Возможная причина ошибки

Детали события	Event details	Возможная причина ошибки
Сервер не отвечает	No response from server	1. Инициатор VPN-соединения отправляет запрос на подключение к VPN-серверу и не получает ответ в течение настроенного времени ожидания. Возможные причины: • Некорректный IP-адрес VPN-сервера в настройках клиентских правил на инициаторе соединения. • Неверный адрес VPN-сервера определяется на DNS-сервере. • На VPN-сервере не открыты порты 500, 4500. • На VPN-сервере не найдено активное правило подключения, подходящее по параметрам: ◦ протокол; ◦ режим IKE; ◦ IP-адрес источника или назначения; ◦ пользователь. • Высокая загрузка VPN-сервера. • Произошла перезагрузка VPN-сервера без сохранения состояния IKE_SA. • Потеря пакетов из-за перегрузки сети 2. После истечения таймера механизма DPD система отправляет первоначальный DPD-запрос. В случае отсутствия ответа и исчерпания всех попыток проверки клиент фиксирует недоступность VPN-сервера. Возможные причины: • На VPN-сервере не открыты порты 500, 4500. • Высокая загрузка VPN-сервера. • Произошла перезагрузка VPN-сервера без сохранения состояния IKE_SA. • Потеря пакетов из-за перегрузки сети. 3. Ошибка в процессе пересоздания ключей (rekeying) для IKE- или ESP-туннеля: VPN-сервер не ответил на запрос. Возможные причины: • Потеря сетевой связности. • Высокая загрузка VPN-сервера. • Произошла перезагрузка VPN-сервера без сохранения состояния IKE_SA. • Потеря пакетов из-за перегрузки сети
Ошибка подключения: некорректное имя сервера	Invalid server name	Доменное имя VPN-сервера, указанное в параметрах подключения инициатора VPN-соединения, не определяется DNS-сервером. Вероятные причины: • Неверно указано доменное имя VPN-сервера в параметрах подключения на узле-инициаторе соединения. • На DNS-сервере не определено доменное имя VPN-сервера
Ошибка подключения: некорректные параметры аутентификации клиента	VPN client connection error — wrong client auth	Ошибка подключения по IKEv2. Узел-инициатор соединения не прошел аутентификацию на VPN-сервере. Возможные причины: • неверно указан общий ключ (PSK) в настройках подключения; • VPN-сервер сопоставил идентификатор клиента с другой политикой, где задан другой общий ключ
Тайм-аут фазы 1. Используется неверный общий ключ	Phase 1 timeout. Incorrect shared key	Ошибка установления IPsec-соединения с использованием протоколов IPsec/L2TP Возможные причины: • В параметрах VPN-подключения указано неверное значение общего ключа. • Не совпадают параметры фазы 1 IKE
Ошибка подключения по протоколу IPsec/L2TP: неверный пароль	VPN client connection error IPsec/L2TP: incorrect password	Ошибка при установлении соединения с протоколами IPsec/L2TP. Возможные причины: • На VPN-сервере создана, но не включена учетная запись для аутентификации узла-инициатора соединения. • Учетная запись для аутентификации узла-инициатора соединения на VPN-сервере не связана с политикой VPN. • На VPN-сервере не настроен профиль аутентификации с локальным пользователем для аутентификации узла-инициатора соединения . • Несовпадение пароля учетной записи на VPN-сервера и в параметрах соединения на узле-инициаторе. • На VPN-сервере нет свободного IP-адреса для клиента
Настройки безопасности VPN-клиента несовместимы с настройками сервера	VPN client and VPN server security settings are not compatible	Ошибка при установлении соединения с протоколами IKEv2 и IPsec/L2TP. Возможные причины: • Несоответствие параметров соединения на VPN-сервере и узле-инициаторе соединения: ◦ Группы Диффи-Хеллмана не совпадают. ◦ Настройки безопасности первой фазы не совпадают. ◦ Настройки безопасности второй фазы не совпадают
Ошибка подключения VPN-клиента — некорректные параметры аутентификации сервера	VPN client connection error — wrong server auth	Ошибка при установлении соединения с протоколами IKEv2. Неуспешная проверка цифровой подписи VPN-сервера в сообщении IKE_AUTH, в результате чего подлинность сервера не подтверждена
Аутентификация клиента невозможна: не получен HASH_I	Client authentication failed: HASH_I not received	Ошибка при установлении соединения по протоколу IKEv1. Значение HASH_DATA, полученное от VPN-сервера, не совпадает со значением, вычисленным на стороне инициатора соединения. Возможные причины: • повреждение пакета при передаче; • потеря предыдущего сообщения, влияющего на вычисление HASH_DATA; • использование некорректного значения общего ключа; • попытка подмены или иного вмешательства в процесс обмена сообщениями
Отсутствие ключевой информации в ответе сервера. Вероятно не совпадает общий ключ	Missing key exchange in server response. Highly likely incorrect shared key	Ошибка при установлении соединения по протоколу IKEv2. В сообщении, полученном от VPN-сервера, отсутствует обязательный payload Key Exchange (KE)

Детали события	Event details	Возможная причина ошибки
Ошибка декодирования сообщения сервера, хэш неверный	Error decoding server message, hash is invalid	Ошибка при установлении соединения по протоколу IKEv2. Инициатор соединения выполняет проверку целостности сообщения, полученного от VPN-сервера, путем вычисления значения Integrity Check Value (ICV) и сравнения его с полученным значением. При несовпадении значений проверка целостности завершается неуспешно, и соединение не устанавливается. Возможные причины: • повреждение или потеря пакетов при передаче (в том числе при фрагментации); • потеря предыдущего сообщения, влияющего на состояние обмена
Настройки безопасности VPN-клиента несовместимы с настройками сервера	VPN client and VPN server security settings are not compatible	Ошибка при установлении соединения по протоколу IKEv1. Параметры защищаемых подсетей (local/remote networks), настроенные на VPN-сервере и узле-инициаторе соединения, не совпадают, в результате чего не удается согласовать параметры IPsec-туннеля
Несовпадение идентификаторов	Incompatible identifiers	Ошибка при установлении соединения по протоколу IKEv2. На этапе согласования IPsec SA клиент отправляет сообщение IKE_AUTH с селекторами трафика (TSi/TSr). VPN-сервер сверяет полученные TSi/TSr с настройками локальных подсетей. Если ни одна подсеть не может быть согласована, VPN-сервер отправляет сообщение INFORMATIONAL со значением Notify payload TS_UNACCEPTABLE, и соединение не устанавливается. Причина: Подсети, настроенные на узле-инициаторе соединения и VPN-сервере, не совпадают
Отсутствие идентификатора в ответе сервера	Missing identifier in server response	Ошибка при установлении соединения по протоколу IKEv1. Узел-инициатор соединения не получил обязательный идентификатор VPN-сервера (IDr) в ответном пакете IKE. В результате невозможна проверка подлинности VPN-сервера, и соединение не устанавливается. Возможные причины: • повреждение или потеря пакетов при передаче; • несоответствие режима IKE в параметрах соединения на узле-инициаторе и на VPN-сервере; • неправильное значение общего ключа в параметрах подключения
Ошибка выделения IP-адреса на сервере	Error allocating IP address from VPN server	Не удалось получить IP-адрес от VPN-сервера. Узел-инициатор соединения не получил свободный IP-адрес от VPN-сервера, поэтому соединение не может быть установлено. Проверьте параметры подключения на VPN-сервере и наличие свободных IP-адресов в пуле

VPN в режиме полного туннелирования

Product: NGFW
Technology: VPN
Version: 7.x, 7.5.x

VPN в режиме полного туннелирования (full tunnel) — это способ подключения, при котором весь сетевой трафик со стороны VPN-клиента, включая обращения к корпоративным системам и к внешним интернет-ресурсам, передается через защищенный VPN-туннель и обрабатывается на VPN-сервере. При таком подходе трафик не разделяется на корпоративный и интернет-трафик — весь поток данных проходит через VPN.

В UserGate NGFW режим полного туннелирования может применяться в сценариях site-to-site VPN с использованием протокола IPsec/IKEv2.

Администратору филиала не нужно поддерживать список корпоративных подсетей — весь трафик по умолчанию передается в туннель, а дальнейшую маршрутизацию VPN-сервер головного офиса выполняет самостоятельно: в свои локальные сети, в другие филиалы или в интернет.

Основные преимущества режима полного туннелирования:

- Полный контроль трафика.
- Единая политика безопасности.
- Централизованное журналирование.

К недостаткам сценария можно отнести повышенную нагрузку на VPN-сервер головного офиса и возможное увеличение сетевых задержек.

Принцип работы

На этапе согласования защищенного канала узел-инициатор соединения (VPN-клиент) запрашивает для селектора трафика VPN-сервера (TSr) значение 0.0.0.0/0, которое принимается VPN-сервером. На узле-инициаторе изменяется таблица маршрутизации: маршрут по умолчанию назначается через VPN-интерфейс, и весь исходящий трафик направляется через корпоративный VPN-сервер. При этом доступ к самому VPN-серверу сохраняется по прямому маршруту вне туннеля.

При разрыве VPN-соединения — по инициативе пользователя, по команде сервера или по иной причине — узел-инициатор завершает VPN-сессию и восстанавливает исходный маршрут по умолчанию.

Настройка режима полного туннелирования на UserGate NGFW

Для создания VPN-подключения необходимо выполнить настройку обоих граничных узлов защищенного соединения: VPN-сервера и узла-инициатора соединения (VPN-клиента).

Настройка VPN-сервера

Настройку VPN-сервера выполните по алгоритму, описанному в разделе « Настройка UserGate NGFW в качестве узла-ответчика ».

Особенности настройки для режима полного туннелирования:

- На VPN-сервере должны быть настроены маршруты в корпоративные сети, сети филиалов и в интернет.
- Должны быть созданы правила сетевых политик, разрешающие доступ к необходимым сетевым ресурсам.
- Настроено правило подключения site-to-site с протоколом IKEv2 с ограничением по IP-адресам. Разрешена соответствующая зона источника.
- Создано правило аутентификации site-to-site IKEv2, в котором:
  - TSr (Local subnets) = 0.0.0.0/0 — VPN-сервер принимает весь трафик по умолчанию от удаленных шлюзов, использующих такую политику.
  - Для удаленных сетей может быть активирована опция «Не проверять сети инициатора», при которой VPN-сервер принимает любые TSi (Remote subnets). Это упрощает конфигурацию.
  - Если опция «Не проверять сети инициатора» отключена, необходимо явно указать подсети, которые VPN-сервер будет проверять при получении трафика от узла-инициатора. Эти подсети добавятся в таблицу маршрутизации VPN-сервера. В этом случае VPN-сервер согласует только те подсети, объявленные узлом-инициатором, которые полностью совпадают с указанными.

Настройка узла-инициатора (VPN-клиента)

Настройку узла-инициатора выполните по алгоритму, описанному в разделе « Настройка UserGate NGFW в качестве узла-инициатора подключения ».

Особенности настройки для режима полного туннелирования:

- До установления VPN-соединения VPN-сервер должен быть доступен согласно текущей таблице маршрутизации (через шлюз по умолчанию, другой L3-шлюз или по L2 — в зависимости от выбранного варианта).
- Должно быть создано правило подключения с протоколом IKEv2 со следующими параметрами:
  - Remote subnets (TSr): 0.0.0.0/0;
  - Local subnets (TSi): указываются только те подсети, которые разрешены на VPN-сервере согласно действующей политике.
- VPN-клиент выполняет роль шлюза по умолчанию для всех локальных подсетей.

Раздельное туннелирование для UserGate Client

Technology: VPN
Version: 7.x, 7.5.x
Product: NGFW

Режим раздельного туннелирования (split tunnel) — это способ удаленного подключения, при котором трафик VPN-клиента разделяется на два потока:

- Часть трафика идет через VPN-туннель (например, доступ к корпоративным ресурсам).
- Остальной трафик идет напрямую через обычное интернет-соединение, минуя VPN.

Принцип работы

Таблица маршрутизации устройства пользователя с установленным ПО UserGate Client модифицируется при установлении VPN-соединения в соответствии с настроенными на VPN-сервере UserGate NGFW параметрами маршрутизации клиента. После завершения VPN-сессии локальные настройки маршрутизации на компьютере пользователя возвращаются в исходные.

При установлении VPN-соединения в таблицу маршрутов клиента добавляются два новых маршрута. Они необходимы для сохранения подключения к VPN-серверу во всех сценариях:

- Маршрут к шлюзу локальной сети. Добавляется через IP-адрес локального интерфейса в качестве шлюза.
- Маршрут к VPN-серверу.
  - Добавляется через IP-адрес локального интерфейса в качестве шлюза, если адрес VPN-сервера находится в адресном пространстве локальной сети.
  - Добавляется через IP-адрес шлюза локальной сети в качестве шлюза в случае если адрес VPN-сервера не находится в адресном пространстве локальной сети.

Локальные маршруты в обход VPN, изначально прописанные на устройстве пользователя, удаляются на время работы VPN. После отключения VPN-соединения эти маршруты возвращаются.

Настройка режима раздельного туннелирования на UserGate NGFW

В веб-консоли UserGate NGFW вы можете настроить различные сценарии работы режима раздельного туннелирования. Для этого перейдите в раздел **Настройки → VPN-сервер → Политики VPN.** В свойствах политики удаленного доступа для UserGate Client выберите вкладку **Маршруты для UserGate Client**.

Рассмотрим подробнее возможные сценарии настроек раздельного туннелирования.

a) Если поставлен флажок **Все маршруты**, в таблицу маршрутизации клиента будет добавлен маршрут по умолчанию (default route) вида 0.0.0.0/0 → VPN-шлюз. Имеющийся ранее маршрут по умолчанию будет удален из таблицы.

b) Если в поле **Включить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида n.n.n.n/c → VPN-шлюз с гарантированно минимальной метрикой 2.

c) Если в поле **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то в таблицу маршрутизации клиента будет добавлен маршрут по умолчанию вида 0.0.0.0/0 → VPN-шлюз. Имеющийся ранее маршрут по умолчанию будет удален из таблицы. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.

d) Если в обоих полях **Включить маршруты** и **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида n.n.n.n/c → VPN-шлюз с гарантированно минимальной метрикой 2. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.

e) Если на вкладке нет никаких настроек, то в таблицу маршрутизации клиента добавляется VPN-маршрут вида 0.0.0.0/0 ➜ VPN-шлюз с метрикой больше, чем у имеющегося маршрута по умолчанию. Имеющийся маршрут по умолчанию при этом не удаляются и маршруты для UserGate MC, UserGate NGFW, VPN-сервера не создаются.

f) Если поставлен флажок **Ограничить доступ к локальной сети**, то для каждой подсети локального интерфейса создается копия маршрута через VPN-шлюз с гарантированно минимальной метрикой 2. Такие же копии маршрутов создаются для всех адресов, которые имеют тип local interface.

В зависимости от сценариев настроек метрики для VPN-маршрутов broadcast- и multicast-адресов получают следующие значения:

- Лучшая метрика среди соответствующих адресов — для сценариев a) и c);
- Гарантированно худшая метрика 10 000 — для сценариев b) и d).

В зависимости от режима работы устройство пользователя с установленным ПО UserGate Client осуществляет коммуникацию либо с UserGate MC, либо с UserGate NGFW. С этой целью создается отдельный маршрут для соответствующего IP-адреса в обход VPN. Такой маршрут не создается для сценария e) и в случае, когда VPN-клиент и UserGate MC или UserGate NGFW находятся в одной сети.

Особенности конвертации правил VPN при обновлении до версии 7.5.x

Version: 7.x
Product: NGFW

В UserGate NGFW версии 7.5.0 была переработана логика построения VPN-правил. Теперь правила реализованы в виде гибкой модульной структуры, основанной на новых настраиваемых объектах. Подробнее о структуре правил VPN — в разделе «Настройка VPN (версия 7.5.0 и выше)».

При обновлении UserGate NGFW до версии 7.5.x с рекомендованных предыдущих версий выполняется автоматическая конвертация существующих VPN-правил в новый формат.

В этой статье рассматриваются особенности конвертации VPN-правил и сценарии взаимодействия узлов с разными версиями ПО в режиме site-to-site VPN.

Увеличение количества правил после конвертации

В процессе конвертации количество объектов настройки VPN на обновленном узле может увеличиться по сравнению с исходной конфигурацией. Это связано с тем, что одно правило старого формата в ряде случаев преобразуется в несколько объектов нового формата.

Для протоколов L2TP/IPsec и IPsec/IKEv2 отдельные серверные правила могут быть разделены на несколько объектов настройки VPN — в зависимости от типа подключения или используемого метода аутентификации.

Например:

- Если в старой модели был настроен серверный профиль безопасности с протоколом IPsec/IKEv2, а параметр **Режим аутентификации** имел значение **Любой**, при конвертации автоматически будут созданы два отдельных правила аутентификации: с режимами PKI и AAA.
- Если в старой модели использовался серверный профиль безопасности с протоколом L2TP/IPsec, при конвертации автоматически будут созданы отдельные правила аутентификации для каждого типа подключения: site-to-site и remote access.

После завершения конвертации рекомендуется проверить автоматически созданные правила и удалить избыточные объекты.

Совместимость версий ПО узлов для site-to-site VPN-соединений

В таблице ниже рассмотрены варианты организации site-to-site VPN-соединений по протоколам L2TP/IPsec, IPsec only/IKEv1, IPsec/IKEv2 с учетом версий ПО узла-инициатора и узла-ответчика.

При планировании обновления узлов, использующих протокол L2TP/IPsec для защищенного соединения офисов, до версии 7.5.0 или выше необходимо учитывать совместимость версий ПО узла-инициатора и узла-ответчика.

Рекомендуемый порядок обновления:

1. Обновите ПО узла-инициатора VPN-соединения до версии 7.5.0 или выше.
2. Убедитесь, что VPN-соединение с узлом-ответчиком, работающим на более ранней версии ПО, по-прежнему устанавливается.
3. Обновите ПО узла-ответчика до версии 7.5.0 или выше.

Рекомендуемый порядок обновления позволяет сохранить возможность установления VPN-соединения по протоколу L2TP/IPsec на промежуточном этапе обновления.

Протокол	Инициатор соединения (версия ПО)	Ответчик (версия ПО)	Способ аутентификации	Возможность соединения	Условия и ограничения
L2TP/IPsec	6.1.9	7.5.1	PSK	-	Сценарий не поддерживается. VPN-соединение установлено не будет
	7.4.3	7.5.1	PSK	-	Сценарий не поддерживается. VPN-соединение установлено не будет
	7.5.1	6.1.9	PSK	+	Подключение к VPN-серверу будет выполняться без дополнительной настройки параметров идентификации, поскольку в старой модели VPN-правил проверка этих параметров не выполняется. Настройка VPN-сервера версии ниже 7.5.0 выполняется в соответствии с документацией для установленной на нем версии ПО. Подробнее о настройке VPN-сервера — в разделе «VPN для защищенного соединения офисов (site-to-site VPN) » руководства администратора UserGate NGFW 6.1.9
	7.5.1	7.4.3	PSK	+	Подключение к VPN-серверу будет выполняться без дополнительной настройки параметров идентификации, поскольку в старой модели VPN-правил проверка этих параметров не выполняется. Настройка VPN-сервера версии ниже 7.5.0 выполняется в соответствии с документацией для установленной на нем версии ПО. Подробнее о настройке VPN-сервера — в разделе «VPN для защищенного соединения офисов (Site-to-Site VPN) » руководства администратора UserGate NGFW 7.x
	7.5.x	7.5.x	PSK	+	После обновления узла-инициатора и узла-ответчика до версии 7.5.x для поддержки подключений по протоколу L2TP/IPsec необходимо вручную настроить параметры **Тип идентификации** и **Значение идентификации** для обеих сторон соединения. Параметры указываются: • в правиле аутентификации VPN-сервера (**Настройки → VPN-сервер → Правила аутентификации**); • в свойствах клиентского подключения (**Настройки → VPN site-to-site client → Подключения клиента**). После настройки параметров необходимо убедиться в успешном установлении VPN-подключения
IPsec only / IKEv1	6.1.9	7.5.1	PSK	+	Серверное правило VPN, созданное в старой модели с привязанным профилем безопасности с протоколом IPsec only/IKEv1 и без указания VPN-подсети (значение **Не использовать** в поле **Сеть VPN**), не будет сконвертировано при обновлении ПО узла-ответчика. Для успешной конвертации перед обновлением устройства укажите в правиле VPN-подсеть. Значение параметра **Подсети для Cisco VPN** в клиентском правиле на узле-инициаторе версии 6.1.9 должно соответствовать значениям **Peer networks (ID)**, указанным в параметрах фазы 2 при настройке правила аутентификации на узле-ответчике версии 7.5.1
	7.4.3	7.5.1	PSK	+	Серверное правило VPN, созданное в старой модели с привязанным профилем безопасности с протоколом IPsec only/IKEv1 и без указания VPN-подсети (значение **Не использовать** в поле **Сеть VPN**), не будет сконвертировано при обновлении ПО узла-ответчика. Для успешной конвертации перед обновлением устройства укажите в правиле VPN-подсеть. Значения параметров **Локальная подсеть** и **Удаленная подсеть** в клиентском профиле безопасности на узле-инициаторе версии 7.4.3 должны соответствовать значениям параметра **Peer networks (ID)**, указанным в параметрах фазы 2 при настройке правила аутентификации на узле-ответчике версии 7.5.1. Для маршрутизации используются подсети, заданные в параметрах правил. Использование системных статических или динамических маршрутов невозможно. Подключение к VPN-серверу будет выполняться без дополнительной настройки параметров идентификации, поскольку в новой модели VPN-правил проверка этих параметров не выполняется
	7.5.1	6.1.9	PSK	-	VPN-сервер версии 6.1.9 не поддерживает работу в роли ответчика для соединения по протоколу IPsec only / IKEv1
	7.5.1	7.4.3	PSK	+	Значения параметров **Peer networks ID** для локальной и удаленной подсетей, указанные при настройке параметров фазы 2 в подключении клиента про протоколу IPsec only / IKEv1 на узле-инициаторе должны соответствовать значениям параметра **Подсети для VPN**, указанным в свойствах серверного профиля безопасности на узле-ответчике

Протокол	Инициатор соединения (версия ПО)	Ответчик (версия ПО)	Способ аутентификации	Возможность соединения	Условия и ограничения
IKEv2	7.4.3	7.5.1	PKI	+	При обновлении ПО узла-ответчика до версии с новой моделью VPN (7.5.0 и выше) серверные правила с протоколом IKEv2 сконвертируются в правила удаленного доступа (тип политики VPN — RA native) с выдачей IP-адреса узлу-инициатору для совместимости со старой моделью VPN на подключаемых узлах. На узле-инициаторе с версией ПО 7.4.3 в свойствах клиентского правила в поле **Адрес сервера** необходимо указывать IP-адрес узла-ответчика. Если указать доменное имя узла, соединение не установится. Если на узле-ответчике версии 7.5.0 или выше необходимо создать новое правило подключения для узлов-инициаторов со старой моделью VPN (версии ниже 7.5.0), настройку серверных правил необходимо выполнить следующим образом: 1. При создании правила подключения в разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите **IKE**. В параметрах правила выберите протокол **IKEv2**. 2. При создании правила аутентификации в разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить**, выберите **Удаленный доступ** и далее выберите **IKEv2**. В параметрах правила укажите режим аутентификации **PKI**. 3. При создании политики VPN в разделе **Настройки → VPN-сервер → Политики VPN** нажмите **Добавить**, выберите **Удаленный доступ** и далее выберите **Clients**. В параметрах политики добавьте правило аутентификации из пункта 2 и укажите пользователя (должен соответствовать пользователю в сертификате),VPN-интерфейс, диапазон IP-адресов и маску для подключения узлов-инициаторов со старой моделью VPN. Подробнее о настройке правил для удаленного доступа — в разделе « Настройка VPN для удаленного доступа в сеть ». Сети, расположенные за VPN-сервером, передаются узлу-инициатору средствами протокола. Для обеспечения обратной маршрутизации к сетям, расположенным за узлом-инициатором, на узле-ответчике необходимо настроить статические маршруты через установленное VPN-соединение
	7.5.1	7.4.3	PKI	+	Узел-инициатор версии 7.5.1 работает в режиме совместимости со старой моделью VPN, используемой узлом-ответчиком версии 7.4.3. На узле-инициаторе должны быть настроены следующие параметры: • туннельный интерфейс должен использовать динамический режим назначения IP-адреса; • в параметрах подключения клиента по протоколу IKEv2 должен быть поставлен флажок **Проверять IP на VPN-сервере** (подробнее о параметре — в разделе «Настройка VPN для защищенного соединения офисов »). На узле-ответчике используется site-to-site правило IKEv2 с выдачей IP-адреса подключившемуся узлу. Сети, расположенные за VPN-сервером, передаются узлу-инициатору средствами протокола. Для обеспечения обратной маршрутизации к сетям, расположенным за узлом-инициатором, на узле-ответчике необходимо настроить статические маршруты через установленное VPN-соединение
	7.5.x	7.5.x	PKI или PSK	+	Новая конфигурация site-to-site подключения. Для установления site-to-site VPN-соединения по протоколу IKEv2 пользователь должен настроить VPN на обеих сторонах. На узле-инициаторе необходимо создать S2S-подключение IKEv2 и указать: • адрес VPN-сервера; • способ аутентификации — PSK или сертификат; • параметры аутентификации; • локальные сети и сети за VPN-сервером (Traffic Selectors). На узле-ответчике необходимо создать S2S-правило IKEv2, настроить соответствующий способ аутентификации и указать подсети за VPN-шлюзами на обеих сторонах соединения. Трафик-селекторы на узле-инициаторе и узле-ответчике должны быть согласованы. Пример настройки site-to-site VPN по протоколу IKEv2 для новой модели VPN — в разделе « Пример настройки site-to-site VPN с IPSec (IKEv2) и аутентификацией посредством сертификатов»

Управление VPN-сессиями

Technology: VPN
Version: 7.x
Product: NGFW

В UserGate NGFW версии 7.5.1 и выше администратор с правами на чтение и запись в разделе **Диагностика и мониторинг** может принудительно завершать выбранные активные VPN-сессии, а также блокировать доступ пользователей к VPN-серверу.

Принудительное завершение активных VPN-сессий

Активные VPN-сессии отображаются в веб-консоли UserGate NGFW в разделе **Диагностика и мониторинг → VPN**.

Для принудительного завершения активных сессий:

1. Выделите необходимые сессии в списке.
2. Нажмите **Завершить сессию**.

Поддерживаются следующие способы множественного выбора:

- Shift + стрелка вверх или вниз;
- Shift + клик мышью;
- Ctrl + клик мышью.

ПримечаниеМаксимально возможное количество одновременно выбранных сессий — 99.

После подтверждения действия выбранные сессии будут корректно завершены VPN-сервером.

ПримечаниеЕсли устройство является инициатором VPN-подключения site-to-site, принудительное завершение соответствующей VPN-сессии недоступно.

В интерфейсе командной строки для просмотра активных VPN-сессий используется следующая команда в режиме диагностики:

Admin@nodename> show vpn-sessions

Для принудительного завершения активных сессий используется команда:

Admin@nodename> clear vpn-sessions <remote-access | site-to-site> [session1 session2 ...]

Журналирование событий завершения сессий

Принудительное завершение VPN-сессии отображается в журнале событий UserGate NGFW как событие «VPN-сессия завершена сервером» с указанием:

- типа соединения;
- названия политики VPN;
- длительности соединения;
- логина пользователя;
- внутреннего IP-адреса;
- имени администратора, выполнившего завершение сессии.

Блокировка пользователей VPN

В некоторых случаях требуется оперативная блокировка доступа пользователей к VPN-серверу, например:

- при компрометации учетных данных;
- утере или краже устройства пользователя;
- выявлении критически опасных уязвимостей VPN-клиента;
- ограничении лицензий или квот.

В веб-консоли UserGate NGFW блокировка доступа пользователей к VPN-серверу может быть выполнена двумя способами:

- через список активных VPN-сессий;
- путем добавления пользователей в список заблокированных.

Чтобы заблокировать пользователей VPN через список активных сессий:

1. Перейдите в раздел **Диагностика и мониторинг → VPN**.
2. Выберите необходимые сессии и нажмите **Заблокировать пользователя**.

После блокировки будут принудительно завершены все активные VPN-сессии выбранных пользователей.

Список пользователей VPN, заблокированных администратором, отображается в разделе **Диагностика и мониторинг → Заблокированные пользователи VPN**. В этом разделе можно добавлять пользователей в список заблокированных, а также разблокировать ранее заблокированных пользователей.

Чтобы добавить пользователей в список заблокированных:

1. Перейдите в раздел **Диагностика и мониторинг → Заблокированные пользователи VPN**.
2. Нажмите **Добавить** и выберите пользователей из списка локальных или доменных пользователей.

После добавления пользователей VPN в список заблокированных все их активные сессии на VPN-сервере будут принудительно завершены.

Чтобы разблокировать пользователей VPN:

1. В разделе **Диагностика и мониторинг → Заблокированные пользователи VPN** выберите нужных пользователей в списке заблокированных.
2. Нажмите **Разблокировать**.

В интерфейсе командной строки для просмотра списка заблокированных пользователей VPN используется следующая команда в режиме диагностики:

Admin@nodename> show blocked-vpn-users

Для добавления локальных пользователей в список заблокированных используется команда:

Admin@nodename> block-vpn-user users [user_name1 user_name2 ...]

Для добавления доменных пользователей в список заблокированных используется команда:

Admin@nodename> block-vpn-user ldap-users connector "Connector name" users [donain\user_name1 domain\user_name2 ...]

Для удаления пользователей из списка заблокированных используется команда:

Admin@nodename> clear blocked-vpn-users users [user_name1 user_name2 ...]

Журналирование событий блокировки

События, связанные с блокировкой пользователей, а также с попытками заблокированных пользователей установить соединение с VPN-сервером отображаются в журнале событий UserGate NGFW.

Добавление пользователей VPN в список блокировки или удаление их из списка отображается как событие «Изменен список заблокированных пользователей VPN» с указанием:

- имени, логина, домена (для доменных пользователей) добавленного или удаленного пользователя;
- времени, когда произошло событие;
- имени администратора, выполнившего действие;
- источника, откуда было инициировано действие (веб-консоль, CLI-консоль, SSH).

Попытки заблокированных пользователей установить соединение с VPN-сервером отображаются как событие «Подключение пользователя к VPN не удалось» с указанием:

- имени, логина, домена пользователя, пытающегося подключиться;
- IP-адреса источника подключения;

- времени события;
- причины отказа в установлении соединения («Пользователь заблокирован»).

Примеры настройки

Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1)

Product: NGFW
Version: 7.x, 7.5.x
Technology: VPN

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема.

Настройка VPN-сервера

Для настройки NGFW1 в качестве VPN-сервера (ответчика) выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

   В разделе **Настройки → Сеть → Зоны** создайте зону WAN и активируйте сервис VPN в параметрах контроля доступа для этой зоны. Подробнее о создании и настройке зон — в разделе «Настройка зон».

2. Создайте зону для VPN-подключений.

   В этом примере воспользуемся уже созданной по умолчанию на узле зоной VPN for Site-to-Site. Подробнее о создании и настройке зон — в разделе «Настройка зон».

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

   В этом примере воспользуемся созданным по умолчанию интерфейсом tunnel3. Подробнее о создании и настройке сетевых интерфейсов — в разделе «Настройка интерфейсов».

4. Настройте параметры аутентификации.

   - Создайте локальную учетную запись, которая будет использоваться для аутентификации узла-инициатора соединения (NGFW2) при установлении L2TP-туннеля. В веб-консоли NGFW1 в разделе **Настройки → Пользователи и устройства → Пользователи** создана локальная учетная запись User for S2S (логин vpn_user_s2s). Для удобства использования все созданные подобные учетные записи могут быть помещены в имеющуюся группу VPN servers, которой будет дан доступ для подключения по VPN. Подробнее о создании учетных записей пользователей и групп — в разделе «Пользователи и группы».
   - Создайте профиль аутентификации. Для примера в разделе **Настройки → Пользователи и устройства → Профили аутентификации** создан профиль local user auth profile, на вкладке метода аутентификации выбран **Локальный пользователь**. Подробнее о профилях аутентификации — в разделе «Профили аутентификации».

5. Создайте правило подключения.

   В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол IKE. Укажите следующие ключевые параметры:

   - На вкладке **Общие**:
     - Укажите название правила подключения.
     - Выберите протокол подключения **IKEv1PSK**.
     - Выберите режим IKE: **Основной**.
     - Укажите значение общего ключа для аутентификации удаленного узла при установлении защищенного соединения IPsec.

   - На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны WAN.

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения.
- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения.
  - Для этого примера настроены параметры работы механизма DPD в режиме **Всегда включено**.
  - Значения параметров криптографии для этого примера оставим заданными по умолчанию.

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Site-to-Site → IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила аутентификации.
  - Выберите профиль аутентификации удаленного сервера-инициатора соединения, созданный на шаге 4.
  - Выберите тип идентификации узлов (**IPv4**).
  - Укажите значения параметров идентификации узла-инициатора и узла-ответчика. В этом примере в качестве значений параметров идентификации указаны IP-адреса внешних интерфейсов узлов NGFW2 и NGFW1.
  - В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

7. Создайте политику VPN-подключения.

В разделе **Настройки → VPN-сервер → Политики VPN** нажмите **Добавить** и выберите **Site-to-Site → IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
    - Укажите название политики VPN-подключения.
    - В блоке **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

- На вкладке **Пользователи** вы можете указать учетные записи или группы, созданные для серверов, которым разрешено подключаться по VPN.
- На вкладке **Подсети для VPN**:
    - Выберите VPN-адаптер, который будет использоваться для установления соединения (tunnel3).
    - Укажите диапазон IP-адресов и маску подсети, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW1 (172.16.0.1), используемому совместно с этой сетью.
    - Оставьте флажок **Использовать системные DNS-серверы** , в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW1.

- На вкладке **Маршруты VPN** вы можете указать маршруты к подсетям за VPN-сервером, передаваемые узлу-инициатору.

Чтобы VPN-сервер (NGFW1) узнал о подсетях за узлом-инициатором соединения, вы можете прописать маршрут к подсетям в свойствах виртуального маршрутизатора VPN-сервера (**Настройки → Сеть → Виртуальные маршрутизаторы**), указав в качестве адреса назначения адрес VPN-туннеля, используемый на NGFW2.

8. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN1.

Подробнее о создании и настройке правил межсетевого экрана — в разделе « Межсетевой экран».

Настройка VPN-клиента

Для настройки NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону для VPN подключений.

В этом примере воспользуемся уже созданной на узле зоной VPN for Site-to-Site.

2. Создайте VPN-интерфейс.

Для этого примера создан VPN-интерфейс tunnel4. Режим получения IP-адреса у этого интерфейса динамический.

3. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN2.

4. Создайте правило подключения к VPN.

В разделе **Настройки → VPN Site-to-Site клиент → Подключение клиента** нажмите **Добавить** и выберите протокол **IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила подключения.
  - Выберите режим IKE: **Основной**.
  - Укажите значение общего ключа для аутентификации узлов. Ключи на VPN-сервере и узле-инициаторе соединения должны совпадать.
  - Выберите параметр идентификации узлов: **IPv4**.
  - Укажите в качестве значений параметров идентификации IP-адреса интерфейсов NGFW2 и NGFW1 из зоны WAN.
  - Укажите логин и пароль учетной записи, созданной на шаге 4 при настройке NGFW1 для аутентификации NGFW2 в процессе установления L2TP-туннеля.

- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения.
    - Для этого примера настроены параметры работы механизма DPD в режиме **Всегда включено**.
    - Значения параметров криптографии для этого примера оставим заданными по умолчанию.

- На вкладке **Фаза 2** укажите параметры второй фазы для установления защищенного канала. Для этого примера оставим значения криптографических параметров, заданные по умолчанию.

5. Создайте клиентское правило.

В разделе **Настройки → VPN Site-to-Site клиент → Клиентские правила** нажмите **Добавить** и укажите следующие ключевые параметры:

- Укажите название клиентского правила.
- Выберите созданное ранее подключение к VPN (ipsec/l2tp).
- Выберите в качестве туннельного интерфейса интерфейс tunnel4, созданный на шаге 2.
- Укажите IP-адрес VPN-сервера (10.72.0.32).

Для инициации соединения включите клиентское правило.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля.

На узлах NGFW1 и NGFW2 в разделе **Диагностика и мониторинг → Мониторинг → VPN** появится информация о новом туннеле.

В разделе **Диагностика и мониторинг → Мониторинг → Маршруты** на узле NGFW2 добавится маршрут в сеть удаленного офиса 10.75.0.0/16 через туннельный интерфейс tunnel4.

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW1.

Со стороны NGFW2.

Сервер и компьютер в сетях обоих офисов доступны друг для друга.

```
Admin@nodename:~$ ip a show ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:91 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.75.0.27/16 brd 10.75.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c91/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.6.1.11
PING 10.6.1.11 (10.6.1.11) 56(84) bytes of data.
64 bytes from 10.6.1.11: icmp_seq=1 ttl=62 time=5.13 ms
64 bytes from 10.6.1.11: icmp_seq=2 ttl=62 time=3.64 ms
64 bytes from 10.6.1.11: icmp_seq=3 ttl=62 time=3.37 ms
^C
--- 10.6.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.370/4.043/5.126/0.772 ms

Admin@nodename:~$ ip a show dev ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:94 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.6.1.11/16 brd 10.6.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c94/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.75.0.27
PING 10.75.0.27 (10.75.0.27) 56(84) bytes of data.
64 bytes from 10.75.0.27: icmp_seq=1 ttl=62 time=6.29 ms
64 bytes from 10.75.0.27: icmp_seq=2 ttl=62 time=6.17 ms
64 bytes from 10.75.0.27: icmp_seq=3 ttl=62 time=8.40 ms
^C
--- 10.75.0.27 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.169/6.952/8.402/1.026 ms
```

Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1) с помощью интерфейса CLI

Product: NGFW
Version: 7.x, 7.5.x
Technology: VPN

В качестве примера для создания site-to-site VPN-туннеля будет рассмотрена следующая схема.

Настройка VPN-сервера

Для настройки узла NGFW 1 в качестве VPN-сервера выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

   Admin@NGFW1# create network zone name WAN enabled-services [VPN]

   Подробнее о командах и параметрах для создания и редактирования зон в CLI — в разделе « Зоны».

2. Создайте зону для VPN-подключений.

   На узле уже создана зона VPN for Site-to-Site. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@NGFW1# show network zone "VPN for Site-to-Site"

name                    : VPN for Site-to-Site
antispoof-enable        : off
antispoof-negate        : off
dos-protection-syn      :
   enabled          : on
   aggregate        : off
   alert-threshold  : 3000
   drop-threshold   : 6000
dos-protection-udp      :
   enabled          : on
   aggregate        : off
   alert-threshold  : 3000
   drop-threshold   : 6000
dos-protection-icmp     :
   enabled          : on
   aggregate        : off
   alert-threshold  : 100
   drop-threshold   : 200
services-access         :
   service          : Any ICMP
   allowed-addresses  : Any
   enabled          : on

   service          : reponse_pages
   allowed-addresses  : Any
   enabled          : on

   service          : DNS
   allowed-addresses  : Any
   enabled          : on

   service          : HTTP Proxy
   allowed-addresses  : Any
   enabled          : on

   service          : Endpoint connect
   allowed-addresses  : Any
   enabled          : on

sessions-limit-enabled  : off
sessions-limit-threshold  : 0
```

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

   Для создания VPN-интерфейса используется команда:

   Admin@ug# create network interface vpn <parameters>

   Подробнее о порядке создания VPN-интерфейса в CLI — в разделе « Интерфейсы».

   На узле изначально уже создан VPN-интерфейс tunnel3, который может быть использован для настройки site-to-site VPN. Установите статический IP-адрес 172.16.0.1 для этого примера.

```
Admin@NGFW1# set network interface vpn tunnel3 ip-addresses [ 172.16.0.1/24 ]
Admin@NGFW1# show network interface vpn tunnel3

type            : vpn
node_name       : cluster
interface-name  : tunnel3
description     : Interface for site-to-site vpn
enabled         : on
netflow-profile  : Undefined
iface-mode      : static
mtu             : 1420
mss             : 0
speed           : 0
zone            : VPN for Site-to-Site
running         : off
master          : off
ip-addresses    : 172.16.0.1/24
```

4. Настройте параметры аутентификации.

   - Создайте локальную учетную запись для аутентификации узла-инициатора соединения при установлении L2TP-туннеля.

     Пример создания учетной записи User for s2s с логином vpn_user_s2s, входящего в группу VPN servers:

     Admin@NGFW1# create users user name "User for s2s" login vpn_user_s2s groups ["VPN servers"] enabled on

     Подробнее о командах и параметрах для создания локальных пользователей в CLI — в разделе « Настройки пользователей».

   - Создайте профиль аутентификации для VPN-пользователей.

     Пример создания профиля аутентификации local user auth profile с аутентификацией по базе данных локально заведенных пользователей:

```
Admin@NGFW1# create users auth-profile name "local user auth profile" auth-methods local-user-auth on
```

Подробнее о порядке создания профилей аутентификации для пользователей в CLI — в разделе « Настройка профилей аутентификации».

5. Создайте правило подключения.

Пример создания правила подключения для протокола IKEv1:

```
Admin@NGFW1# create vpn-server connection-rules ike name ikev1_test_rule protocol ikev1 ike-mode main src-zones [ WAN ] dh-groups [ "Group 2 Prime 1024 bit" "Group 14 Prime 2048 bit" ] security [ SHA1/AES256 SHA256/AES256 ] psk 123
Repeat preshared key:
Admin@NGFW1# show vpn-server connection-rules ike ikev1_test_rule

name               : ikev1_test_rule
type               : ike
protocol           : ikev1
ike-mode           : main
src-zones          : WAN
dh-groups          : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
security           :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256

key-lifetime       : 1 h
dpd-state          : off
dpd-interval       : 60
dpd-max-failures   : 5
```

Подробнее о командах и параметрах для создания правила подключения в CLI — в разделе « Настройка серверных правил VPN».

6. Создайте правило аутентификации.

Пример создания правила аутентификации для протокола l2tp-ipsec:

```
Admin@NGFW1# create vpn-server authentication-rules site-to-site l2tp-ipsec name "s2s ipsec-l2tp auth rule" connection-rules [ "ikev1 conn rule" ] initiator-type ipv4 initiator-value 10.72.0.31 responder-type ipv4 responder-value 10.72.0.32 auth-prc
Admin@NGFW1# show vpn-server authentication-rules site-to-site l2tp-ipsec "s2s ipsec-l2tp auth rule"

name                  : s2s ipsec-l2tp auth rule
connection-rules      : ikev1 conn rule
initiator-type        : ipv4
initiator-value       : 10.72.0.31
responder-type        : ipv4
responder-value       : 10.72.0.32
auth-profile          : local user auth profile
key-lifetime          : 1 h
key-lifesize-enabled  : off
key-lifesize          : 100.0 MB
nat-keepalive         : 0
security              :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256
```

Подробнее о командах и параметрах для создания правила аутентификации в CLI — в разделе « Настройка серверных правил VPN».

7. Создайте политику VPN-подключения.

Политики VPN создаются с помощью синтаксиса языка UASL.

Пример создания правила политики VPN-подключения:

```
Admin@NGFW1# create vpn-server vpn-policy 7 upl-rule \
...OK
...auth_rules("s2s ipsec-l2tp auth rule") \
...vpn_routes(10.75.0.0/16) \
...ip_range("172.16.0.2-172.16.0.254") \
...desc("VPN server policy for S2S IPSec/L2TP connection.") \
...mask(255.255.255.0) \
...use_system_dns(true) \
...enabled(true) \
...type(s2s_l2tp) \
...interface(tunnel3) \
...name("S2S IPSec/L2TP example VPN policy")
```

Подробнее о создании политик VPN в CLI — в разделе « Настройка серверных правил VPN».

Чтобы VPN-сервер (NGFW1) узнал о подсетях за узлом-инициатором соединения, вы можете прописать маршрут к подсетям в виртуальном маршрутизаторе VPN-сервера, указав в качестве адреса назначения адрес VPN-туннеля, используемый на NGFW2.

```
Admin@NGFW1# set network virtual-router default routes new name route1 destination-ip 10.6.0.0/16 gateway 172.16.0.2 enabled on
Admin@NGFW1# show network virtual-router default routes

route1
    name            : route1
    enabled         : on
    destination-ip  : 10.6.0.0/16
    gateway         : 172.16.0.2
    interface       : auto
    metric          : 0
```

8. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN1:

```
Admin@NGFW1# create network-policy firewall 8 upl-rule \
...PASS \
...src.zone = (LAN1, "VPN for Site-to-Site") \
...dst.zone = (LAN1, "VPN for Site-to-Site") \
...rule_log(session) \
...enabled(true) \
...name(allow_lan1_s2s)
```

Подробнее о порядке настройки правил межсетевого экрана в CLI — в разделе « Настройка правил межсетевого экрана».

Настройка VPN-клиента

Для настройки NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону, которой будет принадлежать интерфейс, используемый для подключения по VPN.

На узле изначально создана зона VPN for Site-to-Site. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@NGFW2# show network zone "VPN for Site-to-Site"

name                     : VPN for Site-to-Site
antispoof-enable         : off
antispoof-negate         : off
dos-protection-syn       :
    enabled          : on
    aggregate        : off
    alert-threshold  : 3000
    drop-threshold   : 6000
dos-protection-udp       :
    enabled          : on
    aggregate        : off
    alert-threshold  : 3000
    drop-threshold   : 6000
```

```
dos-protection-icmp         :
    enabled           : on
    aggregate         : off
    alert-threshold   : 100
    drop-threshold    : 200
services-access             :
    service           : Any ICMP
    allowed-addresses   : Any
    enabled           : on

    service           : reponse_pages
    allowed-addresses   : Any
    enabled           : on

    service           : DNS
    allowed-addresses   : Any
    enabled           : on

    service           : HTTP Proxy
    allowed-addresses   : Any
    enabled           : on

    service           : Endpoint connect
    allowed-addresses   : Any
    enabled           : on

sessions-limit-enabled     : off
sessions-limit-threshold   : 0
```

2. Создайте VPN-интерфейс.

Пример создания VPN-интерфейса tunnel4:

```
Admin@NGFW2# create network interface vpn interface-name 4 iface-mode dynamic zone "VPN for Site-to-Site" enabled on
Admin@NGFW2# show network interface vpn tunnel4

type              : vpn
node_name         : cluster
interface-name    : tunnel4
enabled           : on
netflow-profile   : Undefined
iface-mode        : dynamic
mtu               : 1420
mss               : 0
speed             : 0
zone              : VPN for Site-to-Site
running           : off
master            : off
```

3. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN2.

```
Admin@NGFW2# create network-policy firewall 8 upl-rule \
...PASS \
...src.zone = (LAN2, "VPN for Site-to-Site") \
...dst.zone = (LAN2, "VPN for Site-to-Site") \
...rule_log(session) \
...enabled(true) \
...name(allow_lan2_s2s)
```

4. Создайте правило подключения к VPN.

Пример создания правила подключения для протокола IKEv1:

```
Admin@NGFW2# create vpn-client connections l2tp-ipsec name ipsec/l2tp ike-mode main authentication-login vpn_user_s2s authentication-password 123456 initiator-type ipv4 initiator-value 10.72.0.31 responder-type ipv4 responder-value 10.72.0
Repeat preshared key:
Admin@NGFW2# show vpn-client connections l2tp-ipsec ipsec/l2tp

name                    : ipsec/l2tp
ike-mode                : main
authentication-login    : vpn_user_s2s
phase1-key-lifetime     : 1 h
phase2-key-lifetime     : 1 h
key-lifesize-enabled    : off
key-lifesize            : 100.0 MB
initiator-type          : ipv4
initiator-value         : 10.72.0.31
responder-type          : ipv4
responder-value         : 10.72.0.32
dpd-state               : off
dpd-interval            : 60
dpd-max-failures        : 5
dh-groups               : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
phase1-security         :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256

phase2-security         :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256
```

Подробнее о командах и параметрах для создания правила подключения в CLI — в разделе « Настройка клиентских правил VPN».

5. Создайте клиентское правило.

Клиентские правила создаются с помощью синтаксиса языка UASL.

Пример создания клиентского правила для протокола l2tp-ipsec:

```
Admin@NGFW2# create vpn-client rules 4 upl-rule \
...OK \
...server_address("10.72.0.32") \
...connection("ipsec/l2tp") \
...interface(tunnel4) \
...enabled(false) \
...name("ipsec/l2tp")
```

Подробнее о командах и параметрах для создания клиентского правила в CLI — в разделе « Настройка клиентских правил VPN».

Для инициации соединения включите клиентское правило.

```
Admin@NGFW2# set vpn-client rules 4 upl-rule \
...enabled(true)
```

Проверка VPN-соединения

Проверка доступности соседнего узла и маршрута в сеть удаленного офиса.

Со стороны NGFW 1:

```
Admin@NGFW1> show network route

Codes: K - kernel route, C - connected, S - static, R - RIP,
```

```
       O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure
K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:12:57
K>* 10.6.0.0/16 [0/0] via 172.16.0.2, tunnel3, 00:00:16
C>* 10.72.0.0/16 is directly connected, port1, 00:12:57
C>* 10.75.0.0/16 is directly connected, port2, 00:12:57
C>* 10.153.0.0/16 is directly connected, port3, 00:12:57
C>* 172.16.0.0/24 is directly connected, tunnel3, 00:12:57
C>* 172.26.0.0/16 is directly connected, port0, 00:12:57
C>* 172.30.250.0/24 is directly connected, tunnel1, 00:12:57
C>* 172.30.255.0/24 is directly connected, tunnel2, 00:12:57

Admin@NGFW1> ping host 172.16.0.2

PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_req=1 ttl=64 time=1.32 ms
64 bytes from 172.16.0.2: icmp_req=2 ttl=64 time=3.89 ms
64 bytes from 172.16.0.2: icmp_req=3 ttl=64 time=1.71 ms

--- 172.16.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.327/2.311/3.893/1.129 ms
```

Со стороны NGFW 2:

```
Admin@NGFW2> show network route

Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure
K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:08:41
C>* 10.6.0.0/16 is directly connected, port2, 00:08:41
C>* 10.72.0.0/16 is directly connected, port1, 00:08:41
K>* 10.75.0.0/16 [0/0] via 172.16.0.1, tunnel4, src 172.16.0.2, 00:01:18
K>* 172.16.0.1/32 [0/0] is directly connected, tunnel4, 00:01:23
C>* 172.16.0.2/32 is directly connected, tunnel4, 00:01:23
C>* 172.26.0.0/16 is directly connected, port0, 00:08:41

Admin@NGFW2> ping host 172.16.0.1

PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_req=1 ttl=64 time=2.70 ms
64 bytes from 172.16.0.1: icmp_req=2 ttl=64 time=1.76 ms
64 bytes from 172.16.0.1: icmp_req=3 ttl=64 time=3.35 ms

--- 172.16.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.763/2.609/3.359/0.655 ms
```

Проверка установления L2TP-туннеля в журналах узлов.

На NGFW1.

```
Admin@NGFW1> show logs log vpn-server static | grep "LCP connected" -BA 0:23
2026-02-04 13:36:47.063149<0.1074.0> [info][vpn] lcp_fsm:send_connected/1:256 LCP connected
2026-02-04 13:36:47.063159<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:62 PAPResponse with password
2026-02-04 13:36:47.063180<0.1074.0> [info][vpn] lcp_fsm:send_auth_challenge/1:226 PAP protocol selected - wait for client
2026-02-04 13:36:47.064482<0.1074.0> [info][xmlrpc] database:process_server_policy_phase/2:380 server policy "S2S IPSec/L2TP example VPN policy"
2026-02-04 13:36:47.064547<0.1074.0> [warning][xmlrpc] database:login_user_v2/5:449 login user "vpn_user_s2s" ip "10.72.0.31" token
        "35a447c5-a03f-49f4-83d5-3493cd4b983a" guid "c9202ee4-cb35-4d18-91fb-62a67f72aa0e"
2026-02-04 13:36:47.066152<0.1074.0> [info][vpn] lcp_fsm:STATE_OPENED_9/2:984 auth succeed, username <<"vpn_user_s2s">>, guid
        "c9202ee4-cb35-4d18-91fb-62a67f72aa0e", parent pid <0.1073.0>
2026-02-04 13:36:47.066526<0.1074.0> [info][vpn] lcp_fsm:send_auth_response_pap/4:210 send PAP response ID 1 code 2 <<"Willkommen">>
2026-02-04 13:36:47.066581<0.1074.0> [info][vpn] lcp_fsm:send_ccp_configure/2:750 Send CCP configure packet <<1,1,0,6,4,2>>
2026-02-04 13:36:47.066953<0.1074.0> [info][vpn] lcp_fsm:send_ipcp_configure/4:735 Send IPCP configure packet {172,16,0,1}/[{{10,75,0,0},{255,255,0,0}}]
2026-02-04 13:36:47.067352<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',1,1,[{'IPCPOpt_Address',<<0,0,0,0>>},{'IPCPOpt_PriDNS',<<0,0,0,0>>}]}}
2026-02-04 13:36:47.067440<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',255,3,49185,{'LCPProtocolReject',8,1,257}}
2026-02-04 13:36:47.067498<0.1074.0> [error][vpn] lcp_fsm:STATE_OPENED_9/2:1054 Protocol 257 rejected!
2026-02-04 13:36:47.067821<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',2,1,[{'IPCPOpt_Routes',[{{10,75,0,0},{255,255,0,0}}]},{'IPCPOpt_Address',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.068119<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',1,2,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.068174<0.1074.0> [critical][vpn] lcp_fsm:analyze_ipcp_option/2:785 IPClientSuggested {172,16,0,2} IPClientReqTuple {172,16,0,2}
2026-02-04 13:36:47.068258<0.1074.0> [critical][vpn] lcp_fsm:send_ipcp_response/2:881 IPCP ACK! Great deal
        {'IPCPHeader',1,2,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}
2026-02-04 13:36:47.069245<0.1073.0> [warning][vpn] l2tp_fsm:handle_info/3:750 NewIPs [{client_ip,{172,16,0,2}},{server_ip,{172,16,0,1}}] Routes
        [{{10,75,0,0},{255,255,0,0}}]
```

На NGFW2.

```
Admin@NGFW2> show logs log vpn-client static | grep "LCP connected" -BA 0:19
2026-02-04 13:36:47.052244<0.1069.0> [info][vpn] lcp_client:send_connected/1:155 LCP connected, send auth
2026-02-04 13:36:47.056257<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',undefined,undefined,49187,{pap_success,1}}
2026-02-04 13:36:47.056341<0.1069.0> [info][vpn] lcp_client:send_ipcp_configure/4:580 Send IPCP configure packet ip undefined dns undefined
2026-02-04 13:36:47.056330<0.1066.0> [info][vpn] ppp_protocol:decode_ccp/1:387 {'CCPHeader',1,1,<<4,2>>}
2026-02-04 13:36:47.056408<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',undefined,undefined,33021,{'CCPHeader',1,1,<<4,2>>}}
2026-02-04 13:36:47.056668<0.1069.0> [info][vpn] lcp_client:encode_protocol_reject/2:125 send LCP reject protocol "010100060402"
2026-02-04 13:36:47.056903<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',1,1,[{'IPCPOpt_Routes',[{{10,75,0,0},{255,255,0,0}}]},{'IPCPOpt_Address',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.056958<0.1069.0> [critical][vpn] lcp_client:send_ipcp_response/2:628 IPCP ACK! Server ip <<172,16,0,1>>, routes
        [{{10,75,0,0},{255,255,0,0}}]
2026-02-04 13:36:47.057046<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',3,1,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.057072<0.1069.0> [warning][vpn] lcp_client:send_ipcp_response/2:689 Send IPCP answer
        {'IPCPHeader',2,1,[{'IPCPOpt_Routes',[{{10,75,0,0},{255,255,0,0}}]},{'IPCPOpt_Address',<<172,16,0,1>>}]}
2026-02-04 13:36:47.057355<0.1069.0> [info][vpn] lcp_client:send_ipcp_configure/4:580 Send IPCP configure packet ip <<172,16,0,2>> dns <<172,16,0,1>>
2026-02-04 13:36:47.060539<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',2,2,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.060650<0.1069.0> [critical][vpn] lcp_client:send_ipcp_response/2:660 IPCP ACK! Client IP <<172,16,0,2>> dns <<172,16,0,1>>
2026-02-04 13:36:47.061877<0.1069.0> [info][vpn] lcp_client:send_ipcp_response/2:672 AuthToken "a270d112-428f-4d28-8727-354510f99325"
2026-02-04 13:36:47.062790<0.1066.0> [info][vpn] l2tp_client:handle_info/3:729 configure device "tunnel4" static undefined dynamic <<172,16,0,2>>
```

Пример настройки site-to-site VPN с IPSec (IKEv2) и аутентификацией посредством сертификатов

Product: NGFW
Version: 7.x, 7.5.x
Technology: VPN

В качестве примера для создания site-to-site VPN-туннеля будет рассмотрена следующая схема.

Настройка VPN-сервера

Для настройки узла NGFW1 в качестве VPN-сервера (ответчика) выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

   В разделе **Настройки → Сеть → Зоны** создайте зону WAN и активируйте сервис VPN в параметрах контроля доступа для этой зоны. Подробнее о создании и настройке зон — в разделе «Настройка зон».

2. Создайте зону для VPN-подключений.

   В этом примере воспользуемся уже созданной по умолчанию на узле зоной VPN for Site-to-Site. Подробнее о создании и настройке зон — в разделе «Настройка зон».

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

   В этом примере воспользуемся созданным по умолчанию интерфейсом tunnel2. Подробнее о создании и настройке сетевых интерфейсов — в разделе «Настройка интерфейсов».

4. Настройте параметры аутентификации.

   - Импортируйте созданный заранее сертификат VPN-сервера и корневой сертификат. О примерах создания самоподписанных сертификатов — в Приложении.

     В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импорт.** В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его закрытого ключа. В этом же разделе импортируйте корневой сертификат без указания закрытого ключа.

   - Создайте профиль клиентского сертификата в веб-консоли NGFW1. Для этого перейдите в раздел **Настройки → Консоль администратора → Профили клиентских сертификатов** и нажмите **Добавить**. В открывшемся окне укажите название профиля, добавьте импортированный на предыдущем шаге корневой сертификат и выберите поле **Subject altname IPv4** для получения из сертификата узла-инициатора соединения (NGFW2) его IP-адреса.

5. Создайте правило подключения.

   В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол **IKE**. Укажите следующие ключевые параметры:

   - На вкладке **Общие**:
     - Укажите название правила подключения.
     - Выберите протокол подключения **IKEv2**.

- На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны WAN.

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения.
- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Site-to-Site → IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила аутентификации.
  - Выберите режим аутентификации посредством сертификатов (**PKI**).
  - Выберите импортированный на шаге 4 сертификат VPN-сервера.
  - Выберите созданный на шаге 4 профиль клиентского сертификата.
  - Выберите тип идентификации узлов (**IPv4**).
  - Укажите значения параметров идентификации узла-инициатора и узла-ответчика. В этом примере в качестве значений параметров идентификации указаны IP-адреса внешних интерфейсов узлов NGFW2 и NGFW1.
  - В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

7. Создайте политику VPN-подключения.

В разделе **Настройки → VPN-сервер → Политики VPN** нажмите **Добавить** и выберите **Site-to-Site → IPsec**. Укажите следующие ключевые параметры:

- Укажите название правила аутентификации.
- Выберите VPN-адаптер, созданный на шаге 2 (tunnel2).
- В разделе **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

8. Контроль доступа к ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной

на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN1.

Подробнее о создании и настройке правил межсетевого экрана — в разделе « Межсетевой экран».

Настройка VPN-клиента

Для настройки узла NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону для VPN-подключений.

В этом примере воспользуемся уже созданной на узле зоной VPN for Site-to-Site.

2. Создайте VPN-интерфейс.

Для этого примера создан VPN-интерфейс tunnel5. Режим получения IP-адреса у этого интерфейса динамический.

3. Настройте параметры аутентификации.

Импортируйте созданный заранее сертификат VPN-клиента.

В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импорт.** В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его закрытого ключа.

4. Контроль доступа к ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN2.

5. Создайте правило подключения к VPN.

В разделе **Настройки → VPN Site-to-Site клиент → Подключение клиента** нажмите **Добавить** и выберите протокол **IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила подключения.
  - Выберите режим аутентификации с помощью сертификата (**PKI**).
  - Выберите импортированный на шаге 3 сертификат клиента.
  - Выберите параметр идентификации узла (**IPv4**).
  - Укажите в качестве значения параметра идентификации узла IP-адрес интерфейса из зоны WAN (10.72.0.31).

- На вкладке **Фаза 1** укажите параметры фазы 1 для установления защищенного канала IKE SA: Для этого примера оставим значения параметров, заданные по умолчанию

- На вкладке **Фаза 2** укажите параметры второй фазы для установления защищенного канала IPsec SA.
    - Для этого примера оставим значения криптографических параметров, заданные по умолчанию.
    - В разделе **Peer networks** укажите адреса локальных и удаленных подсетей для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В этом примере указываются адреса подсетей LAN2 и LAN1 соответственно

6. Создайте клиентское правило.

В разделе **Настройки → VPN Site-to-Site клиент → Клиентские правила** нажмите **Добавить** и укажите следующие ключевые параметры:

- Укажите название клиентского правила.
- Выберите созданное ранее подключение к VPN (ikev2 pki).
- Выберите в качестве туннельного интерфейса интерфейс tunnel3.
- Укажите адрес VPN-сервера (vpntest.net).

Для инициации соединения включите клиентское правило.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля.

На узлах NGFW1 и NGFW2 в разделе **Диагностика и мониторинг → Мониторинг → VPN** появится информация о новом туннеле.

На узле NGFW1 в разделе **Диагностика и мониторинг → Мониторинг → Маршруты** добавится маршрут в сеть удаленного офиса 10.6.0.0/16 через туннельный интерфейс tunnel2.

На узле NGFW2 в разделе **Диагностика и мониторинг → Мониторинг → Маршруты** добавится маршрут в сеть удаленного офиса 10.75.0.0/16 через туннельный интерфейс tunnel5.

Узлы в сетях обоих офисов доступны друг для друга.

```
Admin@nodename:~$ ip a show ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:91 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.75.0.27/16 brd 10.75.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c91/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.6.1.11
PING 10.6.1.11 (10.6.1.11) 56(84) bytes of data.
64 bytes from 10.6.1.11: icmp_seq=1 ttl=62 time=3.54 ms
64 bytes from 10.6.1.11: icmp_seq=2 ttl=62 time=3.99 ms
64 bytes from 10.6.1.11: icmp_seq=3 ttl=62 time=4.85 ms
^C
--- 10.6.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.536/4.124/4.851/0.545 ms

Admin@nodename:~$ ip a show dev ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:94 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.6.1.11/16 brd 10.6.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c94/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.75.0.27
PING 10.75.0.27 (10.75.0.27) 56(84) bytes of data.
64 bytes from 10.75.0.27: icmp_seq=1 ttl=62 time=6.81 ms
64 bytes from 10.75.0.27: icmp_seq=2 ttl=62 time=6.78 ms
64 bytes from 10.75.0.27: icmp_seq=3 ttl=62 time=4.68 ms
^C
--- 10.75.0.27 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 4.677/6.089/6.808/0.998 ms
```

Пример настройки удаленного доступа в сеть для конечного устройства на Astra Linux

Product: NGFW, UserGate Client
Version: 7.x, 7.5.x
Technology: VPN

Пример создания VPN-подключения между конечным устройством с операционной системой Astra Linux и UserGate NGFW версии 7.5.0.

В этом примере UserGate NGFW выступает в роли VPN-сервера, а компьютер пользователя на Astra Linux с установленным ПО UserGate Client — в роли конечного устройства. Аутентификация пользователя будет происходить с помощью сертификата X.509. Конечному устройству будет передан маршрут к сети за VPN-сервером.

Сначала настройте VPN-сервер, затем настройте VPN-клиент на конечном устройстве и инициируйте подключение к VPN-серверу.

Настройка VPN-сервера

Для настройки UserGate NGFW в качестве VPN-сервера выполните следующие шаги:

1. Разрешите сервис VPN в контроле доступа зоны, из которой будут подключаться конечные устройства.

   В веб-консоли UserGate NGFW в разделе **Настройки → Сеть → Зоны** создайте зону WAN. В параметрах контроля доступа зоны разрешите сервис VPN. Подробнее о создании и настройке зон — в разделе « Настройка зон».

2. Создайте зону для VPN-подключений.

   В этом примере воспользуемся уже созданной по умолчанию зоной VPN for remote access. Подробнее о создании и настройке параметров зон — в разделе « Настройка зон».

3. Создайте VPN-интерфейс для организации туннеля.

   В этом примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом tunnel1, который может быть использован для настройки remote access VPN. Изначально этот интерфейс не активен, его необходимо включить в свойствах интерфейса.

4. Настройте параметры аутентификации:

   - Импортируйте созданные заранее сертификаты: сертификат VPN-сервера и корневой сертификат. Примеры создания самоподписанных сертификатов приведены в Приложении.

     В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импортировать.** В открывшемся окне укажите название сертификата и добавьте созданные ранее файлы сертификата VPN-сервера и его закрытого ключа. В этом же разделе импортируйте корневой сертификат без указания закрытого ключа.

   - Создайте профиль клиентского сертификата в веб-консоли UserGate NGFW. Для этого перейдите в раздел **Настройки → Консоль администратора → Профили клиентских сертификатов** и нажмите **Добавить**. В открывшемся окне укажите название профиля, добавьте импортированный на предыдущем шаге корневой сертификат и выберите **Common-name**, **Subject altname email** или **Principal name** для получения имени пользователя.

   - Создайте профиль аутентификации для пользователей VPN. Подробно о профилях аутентификации — в разделе « Профили аутентификации». Для этого примера был создан профиль аутентификации в домене ADTEST1 через LDAP-коннектор ad16:

5. Создайте правило подключения.

В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол **IKE**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила подключения.
  - Выберите протокол подключения **IKEv2**.

- На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны WAN.

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения от конечных устройств.
- На вкладке **Фаза 1** укажите криптографические параметры фазы 1 согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Удаленный доступ → IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила аутентификации.
  - Выберите импортированный на шаге 4 сертификат VPN-сервера.
  - Выберите созданный на шаге 4 профиль аутентификации пользователя.
  - Выберите режим аутентификации посредством сертификатов (**PKI**).
  - Выберите созданный на шаге 4 профиль клиентского сертификата.
  - В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

7. Создайте политику VPN-подключения.

В разделе **Настройки → VPN-сервер → Политики VPN** нажмите **Добавить** и выберите **Удаленный доступ → UserGate Client**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Поставьте флажок для включения политики VPN.
  - Укажите название правила аутентификации.
  - В разделе **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

- На вкладке **Пользователи** вы можете добавить локальную или доменную учетную запись или группу, которые будут использоваться для аутентификации пользователей.
- На вкладке **Подсети для VPN**
  - Укажите VPN-интерфейс tunnel1, который будет использоваться для подключения.
  - Укажите диапазон IP-адресов, которые будут использованы для подключения. Исключите из диапазона адрес, который назначен VPN-интерфейсу UserGate NGFW, используемому совместно с данной сетью.
  - Укажите маску сети VPN.
  - Оставьте флажок **Использовать системные DNS-серверы** для передачи клиенту туннельного адреса UserGate NGFW в качестве DNS-сервера.

- На вкладке **Маршруты для UserGate Client** укажите параметры маршрутов, передаваемых на конечное устройство с помощью функции раздельного туннелирования.
  - В этом примере на конечном устройстве будет добавлен маршрут к тестовому серверу devsite.ext (10.153.0.5).

8. Настройте контроль доступа к ресурсам.
   - Создайте правило NAT, выполняющее трансляцию IP-адресов при поступлении трафика из зоны VPN for remote access в зону LAN. Правило создается в разделе **Политики сети → NAT и маршрутизация**.
   - При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Настройки → Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны. Для этого примера создано правило межсетевого экрана, разрешающее весь трафик из зоны VPN for remote access в зону LAN.

Настройка VPN-клиента

Предполагается, что ПО UserGate Client уже установлено на конечном устройстве. Подробнее об установке ПО — в разделе « Настройка VPN-соединения на конечном устройстве».

Для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Откройте окно настройки приложения UserGate Client и на вкладке VPN-соединения нажмите **Добавить**.

2. Настройте параметры профиля VPN-соединения:

- Укажите название соединения.
- Укажите IP-адрес или доменное имя VPN-сервера. В этом примере указано доменное имя сервера vpntest.net. Адрес должен быть прописан в серверном сертификате, импортированном на шаге 4 настройки VPN-сервера.
- Выберите протокол для установления VPN-соединения. В этом примере используется протокол **IKEv2**.
- Выберите один из способов аутентификации. В этом примере используется аутентификация посредством сертификатов.
- Выберите заранее созданные файл сертификата пользователя ADTEST1\user, закрытый ключ и введите пароль закрытого ключа.

3. Сохраните параметры профиля, нажав **Сохранить**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения в строке состояния в правом нижнем углу нажмите на значок UserGate Client и в появившемся меню выберите профиль соединения **ikev2 pki**.

В случае успешного подключения на значке UserGate Client появится символ установленного соединения.

Проверка подключения

После установлении VPN-соединения в веб-консоли UserGate NGFW на вкладке **Диагностика и мониторинг** в разделе **Мониторинг →VPN** появилась информация о новом VPN-соединении.

В **Журнале событий** на вкладке **Журналы и отчеты** появилась соответствующая запись.

На конечном устройстве в таблице маршрутизации добавился маршрут к серверу devsite.ext (10.153.0.5) через туннельный интерфейс. Сервер доступен с конечного устройства..