

Table of Contents

Table of Contents	1
Настройка VPN	2
VPN. Общие понятия	3
VPN для защищенного соединения офисов (Site-to-Site VPN)	8
VPN для удаленного доступа клиентов (Remote access VPN)	25

Product: DCFW
Version: 8.x
Technology: VPN

VPN (Virtual Private Network — виртуальная частная сеть) — обобщенное название технологий, позволяющих создавать логические сети (туннели) поверх открытых публичных сетей для обеспечения безопасности коммуникаций.

Для создания VPN необходимо как минимум два сетевых устройства, которые могут идентифицировать друг друга и зашифровать поток данных между собой.

Типы VPN-подключений

UserGate DCFW позволяет создавать VPN-подключения следующих типов:

- VPN для защищенного соединения офисов (**Site-to-Site VPN**). В этом сценарии один узел выступает в роли VPN-сервера, а другой — в роли VPN-клиента. Подключение сервер-сервер позволяет объединить офисы компании в единую логическую сеть.
- VPN для удаленного доступа клиентов в сеть (**Remote access VPN**). В этом сценарии DCFW UserGate выступает в роли VPN-сервера, а устройства пользователей — в роли VPN-клиентов..

Варианты организации защищенных VPN-туннелей

Для создания защищенных VPN-туннелей могут использоваться протоколы L2TP/IPsec(IKEv1), IPsec(IKEv2), IPsec(IKEv1), GRE/IPsec.

L2TP/IPsec VPN

При создании VPN с помощью **L2TP/IPsec**, протокол L2TP ([RFC 3931](#)) создает туннель, в котором пакеты сетевого уровня передаются в кадрах PPP. Поскольку L2TP сам по себе не обеспечивает строгую аутентификацию, конфиденциальность и целостность передаваемых данных, для этих целей используется группа протоколов IPsec ([RFC 6071](#)).

L2TP-туннель создается внутри защищенного IPsec-канала и для его установления необходимо сначала создать защищенное IPsec-соединение между узлами. IPsec в данном случае работает в транспортном режиме и использует протокол ESP (Encapsulating Security Payload) для шифрования L2TP-пакетов.

VPN имеет два уровня инкапсуляции — внутреннюю инкапсуляцию L2TP и внешнюю инкапсуляцию IPsec. Внутренний уровень имеет заголовки L2TP и UDP дополнительно к кадру PPP. Внешний уровень добавляет заголовок и трейлер IPsec ESP. Трейлер проверки подлинности IPsec Auth обеспечивает проверку целостности сообщений и аутентификацию.

Процесс создания VPN состоит из следующих основных этапов:

1. Установление защищенного канала передачи данных.
2. Установление VPN-туннеля.

Установление защищенного канала передачи данных

Для установления защищенного канала передачи данных используется группа протоколов IPsec.

В основе IPsec лежат три протокола:

- Authentication Header (AH).
- Encapsulating security payload (ESP).
- Internet Key Exchange (IKE).

Authentication Header (AH) обеспечивает целостность передаваемых данных, аутентификацию источника информации и защиту от повторной передачи данных. AH не обеспечивает конфиденциальность передаваемых данных, поскольку не осуществляет шифрование. Номер IP-протокола для AH — 51.

Encapsulating security payload (ESP) обеспечивает конфиденциальность передаваемых данных с помощью шифрования, также поддерживается целостность передаваемых данных и аутентификация источника информации. Номер IP-протокола для ESP — 50.

Internet Key Exchange (IKE) — это протокол обмена служебной информацией для согласования и установления ассоциации безопасности (Security Association — SA). Ассоциация безопасности содержит набор параметров защищенного соединения, которые могут использоваться обеими сторонами соединения для взаимной аутентификации и шифрования передаваемых данных. IKE работает по UDP-порту 500.

IPsec может работать в двух режимах:

- Туннельный режим.
- Транспортный режим.

В туннельном режиме протоколом IPsec шифруется весь исходный IP-пакет вместе со своим заголовком. Далее он инкапсулируется внутри дополнительного пакета, который имеет собственный заголовок. Туннельный режим применяется, когда две частные сети передают данные через публичную незащищенную сеть.

В транспортном режиме шифруется только полезная нагрузка IP-пакета, при этом исходный заголовок остается, в него добавляется дополнительная информация. Транспортный режим используется, когда между двумя узлами уже существует IP-связь, но она не обеспечивает защиту передаваемых данных.

В сценарии установления VPN с помощью протоколов L2TP/IPsec туннель между узлами создается протоколом L2TP, при этом IPsec должен обеспечивать безопасность канала. В этом случае IPsec работает в транспортном режиме, а согласование ассоциаций безопасности и установление защищенного канала осуществляется с помощью протокола IKE версии IKEv1 в двух фазах.

В **фазе 1** происходит аутентификация соседних узлов, согласование ассоциации безопасности IKE SA и установление служебного защищенного канала между узлами для обеспечения обмена данными IKE.

Согласуемыми параметрами IKE SA являются:

- Хэш-алгоритмы (MD5, SHA).
- Алгоритмы шифрования (DES, 3DES, AES).

- Параметры времени жизни туннеля.
- Группы Diffie-Hellman.

Для аутентификации узлов канала используется метод общих ключей — pre-shared keys.

Согласование фазы 1 IKEv1 может происходить в двух режимах:

- Основной (Main) режим.
- Агрессивный (Aggressive) режим.

В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации для IKE SA. Вторым обменом (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее.

В агрессивном режиме происходит два обмена сообщениями (всего три сообщения). В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации, и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.

Меньшее количество передаваемых сообщений в агрессивном режиме позволяет достичь более быстрого установления соединения, однако обмен идентификаторами узлов канала осуществляется открытым текстом. Основной режим считается более безопасным, поскольку данные идентификации в основном режиме зашифрованы.

Результатом фазы 1 является согласование двунаправленной ассоциации безопасности IKE SA и установление защищенного служебного канала. Данный канал будет использоваться в фазе 2 для согласования параметров IPsec SA основного канала передачи данных.

В **фазе 2** по защищенному служебному каналу, установленному в фазе 1, происходит согласование IPsec SA для защиты данных, проходящих через канал IPsec.

IKEv1 в фазе 2 имеет один режим, называемый быстрым режимом (Quick mode).

Согласуемыми параметрами IPsec SA являются:

- Алгоритмы шифрования (DES, 3DES, AES).
- Хэш-алгоритмы (MD5, SHA-1, SHA-2).
- Параметры времени жизни SA.

По результатам согласования IPsec SA создается защищенный канал для передачи данных, работающий в транспортном режиме IPsec с инкапсуляцией ESP, имеющий два однонаправленных SA в обе стороны канала.

После его установления служебный канал, созданный в фазе 1, не пропадает - он используется для обновления SA основного.

IPsec SA завершает работу при выключении VPN с одной из сторон соединения или по истечении времени жизни. Тайм-аут по времени жизни возникает при истечении времени жизни ключа или при достижении установленного порога байт данных, прошедших через канал. Когда SA завершает работу, ключи удаляются. Если для передачи данных требуются дополнительные IPsec SA, выполняется новая фаза согласования IKE.

Установление VPN-туннеля

На этом этапе происходит согласование и установление туннеля L2TP между конечными точками SA. Фактическое согласование параметров происходит по защищенному каналу IPsec SA. Протокол L2TP использует UDP-порт 1701.

Когда процесс установления VPN туннеля завершен, пакеты L2TP между конечными точками инкапсулируются с помощью IPsec. Поскольку сам пакет L2TP скрыт внутри пакета IPsec, исходный IP-адрес источника и назначения зашифрован внутри пакета. Кроме того, нет необходимости открывать UDP-порт 1701 на FW между конечными точками, поскольку внутренние пакеты не обрабатываются до тех пор, пока данные IPsec не будут расшифрованы, что происходит только на конечных точках туннеля.

IPsec(IKEv2) VPN

При создании VPN с помощью **IPsec(IKEv2)** защищенный VPN-туннель создается только протоколами группы IPsec с протоколом IKE версии IKEv2 ([RFC 7296](#), [RFC 7427](#)).

В этом сценарии IPsec работает в туннельном режиме, исходные IP-пакеты целиком инкапсулируются и шифруются внутри нового пакета, который имеет свой собственный заголовок и трейлеры.

Подобно IKEv1, IKEv2 также имеет двухэтапный процесс установления защищенного соединения, но при этом происходит меньше обменов сообщениями.

Первый этап известен, как **IKE_SA_INIT**. В двух сообщениях обмена IKE_SA_INIT между соседними узлами происходит согласование параметров ассоциации безопасности IKE SA и установление защищенного служебного канала. Согласуемые параметры IKE SA:

- Хэш-алгоритмы.
- Алгоритмы шифрования.
- Ключи Diffie-Hellman

Каждый узел генерирует seed-key (SKEYSEED) — ключ, который используется для последующей генерации ключей, используемых в IKE SA. Все будущие ключи IKE создаются с помощью SKEYSEED.

Второй этап называется **IKE_AUTH**. На этом этапе происходит проверка подлинности соседних узлов. Два сообщения обмена IKE_AUTH аутентифицируются и шифруются в рамках ассоциации безопасности IKE SA, созданной в обмене сообщениями этапа IKE_SA_INIT.

В конце второго этапа согласования через IKE SA создается дочерняя ассоциация безопасности (CHILD SA) для защищенной передачи данных. **CHILD SA** — это термин IKEv2, подобный IPsec SA для IKEv1. IKEv2 работает через UDP-порты 500 и 4500 (IPsec NAT Traversal).

Дополнительные CHILD SA могут создаваться для организации нового туннеля. Этот обмен называется CREATE_CHILD_SA, в нем могут быть согласованы новые значения групп Diffie-Hellman, новые комбинации алгоритмов шифрования и хэширования.

Аутентификация узлов IPsec туннеля может происходить посредством сертификатов, использующих инфраструктуры открытых ключей (PKI) или с помощью протокола EAP (Extensible Authentication Protocol).

IPsec(IKEv1) VPN

При создании VPN с помощью **IPsec(IKEv1)** защищенный VPN-туннель создается протоколами группы IPsec с протоколом IKE версии IKEv1.

UserGate DCFW в таком сценарии может работать в качестве VPN-клиента и в качестве VPN-сервера.

GRE/IPsec VPN

GRE ([RFC 2784](#)) — это протокол туннелирования, позволяющий инкапсулировать пакеты протоколов различного типа внутри IP-туннелей, благодаря чему создается виртуальный канал «точка-точка» поверх IP-сети. GRE предназначен для управления процессом передачи многопротокольного и группового IP-трафика между двумя и более площадками, между которыми связь может обеспечиваться только по IP. При этом GRE не обеспечивает конфиденциальность и целостность передаваемых данных. Для этих целей совместно с GRE используются протоколы группы IPsec.

При совместном использовании GRE и IPsec могут быть созданы 2 типа соединений: IPsec over GRE и GRE over IPsec.

При использовании соединения IPsec over GRE происходит передача зашифрованного трафика по незащищённому GRE-туннелю, т.е. сначала происходит инкапсуляция IPsec, а затем инкапсуляция GRE. Недостаток IPsec over GRE заключается в том, что не поддерживается передача многоадресных и широковещательных пакетов.

Соединение GRE over IPsec позволяет использовать преимущества GRE (поддержка многоадресной и широковещательной рассылки) и IPsec (передача трафика в зашифрованном виде). При использовании соединения GRE over IPsec происходит инкапсуляция пакетов в GRE, а затем их передача по зашифрованному каналу связи (инкапсуляция IPsec).

Для настройки GRE over IPsec необходимо выполнить следующие шаги:

Параметр	Описание
Шаг 1. Настройка Site-to-Site VPN-соединения.	Подробнее о настройке Site-to-Site VPN-соединения читайте далее в разделе VPN для защищенного соединения офисов (Site-to-Site VPN) .
Шаг 2. Настройка туннеля GRE.	Подробнее о настройке туннельного интерфейса GRE читайте в разделе Интерфейс туннель . Важно! При настройке туннельного GRE интерфейса в качестве адресов источника (локальный IP) и назначения (удалённый IP) должны быть указаны IP-адреса VPN-интерфейсов.

VPN для защищенного соединения офисов (Site-to-Site VPN)

Product: DCFW
Version: 8.x
Technology: VPN

VPN-подключение, позволяющее соединить локальные сети удаленных офисов, называется Site-to-Site VPN.

В этом подключении один межсетевой экран выступает в роли VPN-сервера, а другой — в роли VPN-клиента. Клиент инициирует соединение с сервером. Site-to-Site VPN может быть создан между двумя межсетевыми экранами UserGate, либо между межсетевым экраном UserGate и устройством другого производителя.

При создании Site-to-Site VPN-туннелей используются протоколы L2TP/IPsec(IKEv1), IPsec(IKEv2), IPsec(IKEv1).

Необходимо произвести настройки соответствующих параметров на обоих граничных узлах защищенного соединения — на VPN-сервере, и на VPN-клиенте.

Алгоритм настройки VPN-сервера

Настройка VPN-сервера на DCFW состоит из следующих основных этапов:

1. [Контроль доступа зоны.](#)
2. [Создание зоны для VPN подключений.](#)
3. [Настройка параметров аутентификации.](#)
4. [Создание профиля безопасности VPN.](#)
5. [Создание VPN-интерфейса.](#)
6. [Создание сети VPN.](#)
7. [Создание серверного правила VPN.](#)
8. [Контроль доступа к ресурсам.](#)

Контроль доступа зоны

Необходимо разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

Это можно сделать в веб-консоли администратора, перейдя в раздел **Сеть → Зоны**. Далее в настройках контроля доступа для той зоны, с которой будут подключаться VPN-клиенты, нужно разрешить сервис VPN. Как правило, это зона **Untrusted**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Создание зоны для VPN-подключений

Необходимо создать зону, в которую будут помещены подключаемые по VPN узлы.

В веб-консоли администратора зона создается в разделе **Сеть → Зоны**. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Настройка параметров аутентификации

При организации VPN-туннеля с протоколом **L2TP** необходимо на VPN-сервере создать локальную учетную запись, которая будет использоваться для аутентификации узла, выполняющего роль VPN-клиента. Локальная учетная запись создается в разделе **Пользователи и устройства → Пользователи**. Для удобства использования все созданные подобные пользователи могут быть помещены в имеющуюся группу **VPN servers**, которой будет дан доступ для подключения по VPN. Подробнее о создании учетных записей пользователей и групп читайте в разделе руководства [Пользователи и группы](#).

При создании защищенного соединения **IPsec** возможны следующие методы аутентификация удаленного узла:

- Аутентификация посредством **общего ключа** (Pre-shared key). Используется при выборе протокола **IKEv1** для организации защищенного соединения. Общий ключ задается в настройках профилей безопасности VPN. Он должен совпадать на [VPN-сервере](#) и [VPN-клиенте](#) для успешного подключения.
- Аутентификация посредством **сертификатов**, использующих инфраструктуру открытых ключей (PKI). Используется при выборе протокола **IKEv2** для организации защищенного соединения. Необходимо заранее создать сертификаты сервера и клиента и импортировать их в DCFW. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#).

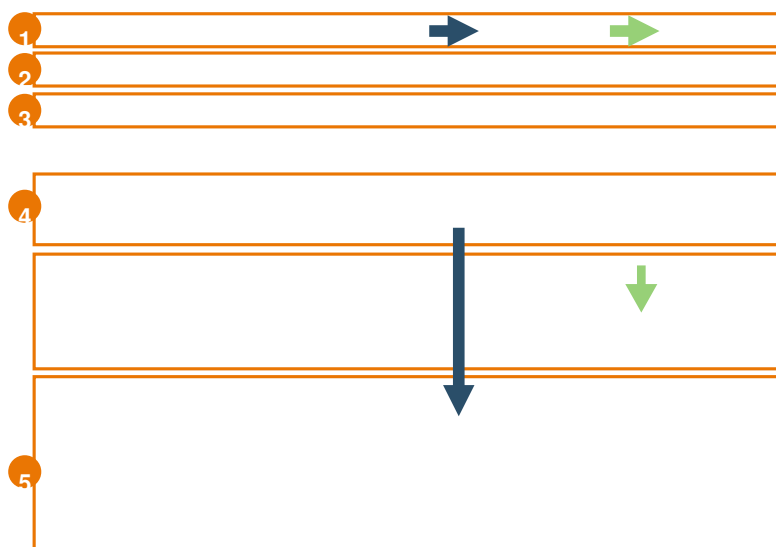
При необходимости аутентификации **пользователей VPN** нужно создать соответствующий профиль аутентификации. Профили аутентификации создаются в разделе **Пользователи и устройства → Профили аутентификации**. Допускается использовать тот же профиль, что используется для аутентификации пользователей с целью получения доступа к сети интернет. Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. Подробнее о профилях аутентификации читайте в разделе руководства [Профили аутентификации](#).

Создание профиля безопасности VPN

В настройках профиля безопасности VPN определяются типы и параметры алгоритмов шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов.

В веб-консоли администратора в разделе **VPN** профили безопасности для узлов, выступающих в роли VPN-сервера и VPN-клиента, настраиваются отдельно:

Для создания профиля безопасности **VPN-сервера** необходимо перейти в раздел **VPN → Серверные профили безопасности**, нажать кнопку **Добавить** и заполнить необходимые поля в свойствах профиля безопасности:



Вкладка **Общие** предназначена для выбора версии протокола VPN и задания параметров аутентификации узлов при установлении защищенного соединения.

1. **Протокол.** Возможны следующие варианты выбора поля:

- **IPsec/L2TP.**
- **IPsec only/IKEV1.**
- **IKEv2.**

2. **Режим работы IKE** (доступно только для IKEv1). Возможны следующие варианты выбора поля:

- **Основной.**
- **Агрессивный.**

3. **Тип идентификации** (параметр IKE local ID). Необходим для идентификации DCFW на соседнем узле при установлении VPN-соединения с оборудованием некоторых производителей. Возможные значения выбора поля:

- **Отсутствует** — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate.
- **IPv4** — IP-адрес узла.
- **FQDN** — адрес узла в формате полностью определенного доменного имени (FQDN).
- **CIDR** — адрес узла в формате бесклассовой адресации (CIDR).
- **Значение идентификации** — значение параметра IKE local ID в формате выбранного ранее типа.

4. Тип аутентификация удаленного узла при установлении защищенного соединения.

- При выборе протокола IKEv1 используется аутентификация с **общим ключом** (Pre-shared key). Необходимо задать общий ключ. Строка должна совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
- При выборе протокола IKEv2 для организации туннеля Site-to-Site возможна аутентификация с помощью сертификатов, использующих инфраструктуру открытых ключей (PKI). Необходимо указать заранее созданные сертификат сервера и профиль клиентских сертификатов. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#). О создании профилей клиентских сертификатов читайте в разделе [Профили клиентских сертификатов](#).

5. **Подсети для VPN.** Задаются при выборе протокола организации VPN-туннеля IPsec only/IKEV1:

- **Локальная подсеть** — IP-адрес разрешенной локальной подсети.
- **Удаленная подсеть** — IP-адрес разрешенной подсети со стороны удаленного узла.

Далее необходимо задать криптографические параметры первой и второй фаз согласования защищенного соединения.

Во время первой фазы происходит согласование и установление IKE SA. Необходимо указать следующие параметры:

6

7

8

9

6. **Время жизни ключа** — по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.

7. Режим работы механизма **Dead peer detection** (DPD) — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны 3 режима работы механизма:

- **Отключено** — Механизм отключен. DPD запросы не отправляются.
- **Всегда включено** — DPD запросы всегда отправляются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отправляются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается.
- **При отсутствии трафика** — DPD запросы не отправляются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отправляются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.

8. **Diffie-Hellman группы** — выбор групп Диффи-Хеллмана, которые будут использоваться для обмена ключами.

9. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Во второй фазе осуществляется выбор способа защиты передаваемых данных в IPsec подключении. Необходимо указать следующие параметры:

10. **Время жизни ключа** — по истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.

11. **Максимальный размер данных, шифруемых одним ключом** — время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии.

12. **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 реер-узла для поддержания сессии NAT активной.

13. **Безопасность** — алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

VPN-интерфейс в веб-консоли администратора создается в разделе **Сеть → Интерфейсы**. Необходимо нажать кнопку **Добавить** и выбрать **Добавить VPN**, далее в настройках VPN-адаптера задать необходимые параметры:

1

2

3

4

5

1. **Включено** — включение/отключение интерфейса.

2. **Название** — название интерфейса, должно быть в виде *tunnelN*, где *N* — это порядковый номер VPN-интерфейса.

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к DCFW, будут также помещены в эту зону. В этом поле указывается зона, созданная ранее на этапе [создания зоны для VPN подключений](#).

4. **Профиль netflow**, используемый для данного интерфейса. Подробнее о профилях netflow читайте в статье [Профили netflow](#). Опциональный параметр.

5. **Алиас/Псевдоним** интерфейса. Опциональный параметр.

6

7

8

6. **Режим** — тип присвоения IP-адреса. Возможные опции выбора — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN), то необходимо использовать статический IP-адрес.

7. **MTU** — размер MTU для выбранного интерфейса. Если пакеты, передаваемые через VPN-туннель, превышают максимальный размер MTU на любом из промежуточных устройств, они могут быть разделены на фрагменты. Это может привести к увеличению задержки и потере

производительности. Путем установки оптимального значения MTU на туннельном интерфейсе можно избежать фрагментации и снизить задержку.

8. Поле добавления **IP-адреса** VPN-интерфейса в случае, если выбран статический режим присвоения адреса.

Создание сети VPN

Сеть VPN определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов.

Сеть VPN в веб-консоли администратора создается в разделе **VPN → Сети VPN**, Необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах VPN-сети:

1

2

1. **Название** сети VPN.

2. **Описание** сети VP. Опциональный параметр.

3

4

5

3. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен **VPN-интерфейсу** DCFW, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.

4. **Маска** сети VPN.

5. Указать **DNS-серверы**, которые будут переданы клиенту, или поставить флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует DCFW.

Важно! Можно указать не более двух DNS-серверов.

6

6. **Маршруты VPN** — маршруты, передаваемые VPN-клиенту в виде бесклассовой адресации (CIDR) или заранее созданного списка IP-адресов.

Вкладка **Маршруты для UserGate client** не используется в сценарии настройки VPN для защищенного соединения офисов (Site-to-Site VPN). Она предназначена для настройки функции раздельного туннелирования для UserGate Client в сценарии удаленного доступа в сеть.

Создание серверного правила VPN

Серверные правила VPN в веб-консоли администратора создаются в разделе **VPN → Серверные правила**. Далее необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах правила:

1

2

3

4

5

6

7

1. **Включено** — включение/отключение правила VPN.

2. **Название** серверного правила VPN.

3. **Описание** серверного правила VPN. Опциональный параметр.

4. **Профиль безопасности VPN** — профиль безопасности, созданный [ранее](#).

5. **Сеть VPN** — сеть, созданная ранее на этапе [создания сети VPN](#). При настройке серверного правила для IPsec-туннеля, когда UserGate является VPN-сервером (указан протокол VPN **IPsec only/IKEV1** в свойствах серверного профиля безопасности) необходимо в данном поле выбрать опцию **Не использовать**.

6. **Профиль аутентификации** — профиль аутентификации для пользователей VPN. Допускается использовать тот же профиль, что используется для аутентификации пользователей с целью получения доступа к сети интернет. Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. При необходимости в разделе **Пользователи и устройства → Профили аутентификации** можно создать профиль аутентификации для пользователей VPN. Подробно о профилях

аутентификации смотрите в разделе [Профили аутентификации](#).

При настройке серверного правила для IPsec-туннеля, когда UserGate является VPN-сервером (указан протокол VPN **IPsec only/IKEV1** в свойствах серверного профиля безопасности) необходимо в данном поле выбрать опцию **Не использовать**.

7. **Интерфейс** — созданный ранее [VPN-интерфейс](#).



8. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**.

Важно! Обработка трафика происходит по следующей логике:

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



9. **Пользователи** — группа учетных записей серверов или отдельные учетные записи серверов, которым разрешено подключаться по VPN.



10 Назначение — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на этапе [контроля доступа зоны](#).

Важно! Для применения различных серверных правил к разным клиентам необходимо использовать параметры *Зона источника* и *Адрес источника*. Параметр *Пользователи* не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.

Примечание При изменении настроек VPN-сервера (изменение серверных правил, изменение профилей безопасности, добавление новых VPN-сетей) не происходит перезагрузка VPN-сервера, благодаря чему ранее установленные активные сессии VPN-клиентов не обрываются. Перезагрузка VPN-сервера и переподключение активных сессий VPN-клиентов может произойти в случае смены IP-адреса туннельного интерфейса VPN-сервера.

Примечание Начиная с версии ПО 7.2.0 трафик, приходящий через VPN-соединение между офисами, маркируется в журналах логинами конкретных пользователей, если они известны, иначе — именем "Unknow".

Контроль доступа к ресурсам

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети, или, например, для предоставления доступа в интернет в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из [зон для VPN-подключений](#) в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в разделе руководства [Межсетевой экран](#).

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, сконфигурированную ранее [зону для VPN-подключений](#).

На VPN-сервере необходимо настроить маршрутизацию для возвратного трафика. Например, для того чтобы VPN-сервер узнал о подсетях клиента, необходимо в свойствах виртуального маршрутизатора (**Сеть → Виртуальные маршрутизаторы**) сервера прописать статический маршрут, указав в качестве адреса назначения адрес VPN-туннеля, используемый на VPN-клиенте. Подробнее о настройках виртуального маршрутизатора читайте в разделе руководства [Виртуальные маршрутизаторы](#).

Алгоритм настройки VPN-клиента

Настройка VPN-клиента на DCFW состоит из следующих основных этапов:

1. [Создание зоны для VPN подключений.](#)
2. [Создание VPN-интерфейса.](#)
3. [Контроль доступа к ресурсам.](#)
4. [Настройки параметров аутентификации.](#)
5. [Создание профиля безопасности VPN.](#)
6. [Создание клиентского правила VPN.](#)

Создание зоны для VPN-подключений

Необходимо создать зону, в которую будут помещены интерфейсы, используемые для подключения по VPN. В веб-консоли администратора зона создается в разделе **Сеть → Зоны**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения по VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

VPN-интерфейс в веб-консоли администратора создается в разделе **Сеть → Интерфейсы**. Необходимо нажать кнопку **Добавить** и выбрать **Добавить VPN**, далее в настройках VPN-адаптера задать необходимые параметры:

1

2

3

4

5

1. **Включено** — включение/отключение интерфейса.

2. **Название** — название интерфейса, должно быть в виде *tunnelN*, где *N* — это порядковый номер VPN-интерфейса. Расположенное ниже поле **Описание** является опциональным.

3. **Зона**, к которой будет относиться данный интерфейс. В этом поле указывается зона, созданная ранее на этапе [создания зоны для VPN подключений](#).

4. **Профиль netflow**, используемый для данного интерфейса. Подробнее о профилях netflow читайте в статье [Профили netflow](#).
Опциональный параметр.

5. **Алиас/Псевдоним** интерфейса. Опциональный параметр.

6

7

6. **Режим** — тип присвоения IP-адреса. Возможные опции выбора — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — **Динамический**. При установлении соединения интерфейсу будет присвоен IP-адрес из диапазона сети VPN, сконфигурированной в настройках VPN-сервера на этапе [создания сети VPN](#).

7. **MTU** — размер MTU для выбранного интерфейса. Если пакеты, передаваемые через VPN-туннель, превышают максимальный размер MTU на любом из промежуточных устройств, они могут быть разделены на фрагменты. Это может привести к увеличению задержки и потере производительности. Путем установки оптимального значения MTU на туннельном интерфейсе можно избежать фрагментации и снизить задержку.

Важно! Если при настройке туннельного интерфейса на стороне VPN-сервера и VPN-клиента был выбран уже созданный для примера один и тот же туннельный интерфейс с настройками по умолчанию, то при подключении клиента к серверу возникнет конфликт IP-адресов. Для корректной работы диапазоны адресов туннельных интерфейсов не должны пересекаться. Необходимо изменить диапазоны адресов на клиенте и сервере на уникальные.

Контроль доступа к ресурсам

При необходимости в разделе **Политики сети → Межсетевой экран** создать разрешающее правило межсетевого экрана, разрешающее трафик между зоной для VPN-подключений и зонами назначения.

Чтобы трафик передавался на сервер из нужной зоны сервера-клиента через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, зону VPN-подключений. Подробнее о создании и настройке правил межсетевого экрана смотрите в разделе руководства [Межсетевой экран](#).

Настройки параметров аутентификации

При создании защищенного соединения **IPsec** с **IKEv2** используется аутентификация посредством **сертификатов**, использующих инфраструктуру открытых ключей (PKI). Созданный ранее сертификат VPN-клиента необходимо импортировать в разделе **UserGate → Сертификаты** на устройстве, исполняющем роль VPN-клиента.

О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#).

Создание профиля безопасности VPN

В настройках профиля безопасности VPN определяются типы и параметры алгоритмов шифрования и аутентификации. В разделе **VPN** веб-консоли администратора профили безопасности для узлов, выступающих в роли VPN-сервера и VPN-клиента, настраиваются отдельно:

Для создания профиля безопасности **VPN-клиента** необходимо перейти в раздел **VPN → Клиентские профили безопасности**, нажать кнопку **Добавить** и заполнить необходимые поля в свойствах клиентского профиля безопасности:

1

2

3

4

5

6

8

7

Вкладка **Общие** предназначена для выбора версии протокола IKE и задания параметров аутентификации узлов при установлении защищенного соединения.

1. **Название** клиентского профиля безопасности.
2. **Описание** клиентского профиля безопасности. Опциональный параметр.
3. **Протокол** — протокол установления VPN канала между двумя сетями. Возможны следующие варианты выбора поля:
 - **IPsec L2TP** — для создания защищенного VPN канала с использованием L2TP и IPsec/IKEv1.
 - **IPsec** — для создания защищенного VPN канала с VPN-сервером с использованием IPsec/IKEv1.
 - **IKEv2 с сертификатом** — для создания защищенного VPN канала с использованием IKEv2 и аутентификацией с помощью сертификата, использующего инфраструктуру открытых ключей (PKI).
4. **Режим работы IKE**. Возможны следующие варианты выбора поля:
 - **Основной**.
 - **Агрессивный**.
5. **Тип идентификации** (параметр IKE local ID). Необходим для идентификации соседнего узла при установлении VPN-соединения с оборудованием некоторых производителей. Возможные значения выбора поля:
 - **Отсутствует** — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate.
 - **IPv4** — IP-адрес узла.
 - **FQDN** — адрес узла в формате полностью определенного доменного имени (FQDN).
 - **CIDR** — адрес узла в формате бесклассовой адресации (CIDR).
 - **Значение идентификации** — значение параметра IKE local ID в формате выбранного ранее типа.
6. Тип аутентификация удаленного узла при установлении защищенного соединения.
 - При выборе протокола **IPsec/L2TP** и **IPsec** используется аутентификация с общим ключом (Pre-shared key). Необходимо задать общий ключ. Строка должна совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
 - При выборе протокола **IKEv2 с сертификатом** для организации туннеля Site-to-Site используется аутентификация с помощью сертификатов, использующих инфраструктуру открытых ключей (PKI). Необходимо указать заранее созданный сертификат клиента. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#).
7. **Аутентификация** — логин и пароль локальной учетной записи, [созданной](#) на VPN-сервере для аутентификации узла, выступающего в роли VPN-клиента при установлении **L2TP** туннеля.

8. Подсети для VPN:

- **Локальная подсеть** — IP-адрес разрешенной локальной подсети.
- **Удаленная подсеть** — IP-адрес разрешенной подсети со стороны удаленного VPN-сервера.

Далее необходимо задать криптографические параметры первой и второй фаз согласования защищенного соединения.

Во время первой фазы происходит согласование и установление IKE SA. Необходимо указать следующие параметры:

9

10

11

12

9. **Время жизни ключа** — по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.

10. Режим работы механизма **Dead peer detection** (DPD) — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны 3 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 есть, 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, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова 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.

11. **Diffie-Hellman группы** — выбор групп Диффи-Хеллмана, которые будут использоваться для обмена ключами.

12. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Во второй фазе осуществляется выбор способа защиты передаваемых данных в IPsec подключении. Необходимо указать следующие параметры:

13

14

15

13. **Время жизни ключа** — по истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.

14. **Максимальный размер данных, шифруемых одним ключом** — время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии.

15. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Создание клиентского правила VPN

Клиентское правило VPN будет инициировать подключение к VPN-серверу. Клиентские правила VPN в веб-консоли администратора создаются в разделе **VPN → Клиентские правила**. Далее необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах правила:

1	
2	
3	
4	
5	
6	

1. **Включено** — включение/отключение данного правила.

2. **Название** клиентского правила.

3. **Описание** клиентского правила. Опциональный параметр.

4. **Профиль безопасности VPN** — созданный ранее [клиентский профиль безопасности VPN](#).

5. **Интерфейс** — созданный ранее [VPN-интерфейс](#).

6. **Адрес сервера** — адрес VPN-сервера (IP-адрес, FQDN), куда подключается данный VPN-клиент.

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

VPN для удаленного доступа клиентов (Remote access VPN)

Product: DCFW
Version: 8.x
Technology: VPN

VPN-подключение, с помощью которого пользователи могут получить защищенный доступ к корпоративной сети компании через Интернет, называется Remote access VPN.

В этом подключении межсетевой экран UserGate (DCFw) выступает в роли VPN-сервера, а устройства пользователей — в роли VPN-клиентов. В качестве клиентского ПО на устройствах пользователей может использоваться UserGate Client, также поддерживаются нативные клиенты большинства популярных операционных систем.

Для организации защищенного подключения используются следующие протоколы:

- L2TP/IPSec(IKEv1);
- IPSec(IKEv2).

Для создания Remote Access VPN необходимо произвести [настройки соответствующих параметров на VPN-сервере](#) (DCFw), а затем [настроить и подключить VPN-клиент](#) на оборудовании пользователя.

Настройка VPN-сервера

Алгоритм настройки VPN-сервера на UserGate DCFw включает в себя следующие основные этапы:

1. [Контроль доступа зоны](#).
2. [Создание зоны для VPN подключений](#).
3. [Настройка параметров аутентификации](#).
4. [Создание профиля безопасности VPN](#).
5. [Создание VPN-интерфейса](#).
6. [Создание сети VPN](#).
7. [Создание серверного правила VPN](#).

Контроль доступа зоны

Необходимо разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

Это можно сделать в веб-консоли администратора, перейдя в раздел **Сеть → Зоны**. Далее в настройках контроля доступа для той зоны, с которой будут подключаться VPN-клиенты, нужно разрешить сервис VPN. Как правило, это зона **Untrusted**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Создание зоны для VPN-подключений

Необходимо создать зону, в которую будут помещены подключаемые по VPN клиенты.

В веб-консоли администратора зона создается в разделе **Сеть → Зоны**. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Настройка параметров аутентификации

1. При создании защищенного соединения **IPsec** возможны следующие методы **аутентификации узлов**:

- Аутентификация посредством **общего ключа** (Pre-shared key). Используется при выборе протокола **IKEv1** для организации защищенного соединения. Общий ключ задается в настройках [профиля безопасности VPN](#). Он должен совпадать на [VPN-сервере](#) и на VPN-клиентах для успешного подключения.
- Аутентификация посредством **сертификатов**, использующих инфраструктуру открытых ключей (PKI). Используется при выборе протокола **IKEv2** для организации защищенного соединения. Необходимо заранее создать сертификаты сервера и клиентов и импортировать их в DCFW и на клиентские компьютеры. Также в DCFW необходимо создать профили клиентских сертификатов. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#). О создании профилей клиентских сертификатов читайте в разделе [Профили клиентских сертификатов](#).

2. Для аутентификации **пользователей VPN** нужно создать соответствующий профиль аутентификации. Профили аутентификации создаются в разделе **Пользователи и устройства → Профили аутентификации**. Допускается использовать тот же профиль, что используется для аутентификации пользователей с целью получения доступа к сети интернет. Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP.

При аутентификации пользователей VPN возможно использование многофакторной аутентификации. Второй фактор может быть получен через одноразовые коды TOTP. VPN с TOTP работает для клиента UserGate Client только с IKEv2 (код вводится в отдельном окне), для других клиентов — только с IKEv1 (код вводится в пароле через двоеточие: *пароль_пользователя:totp_code*).

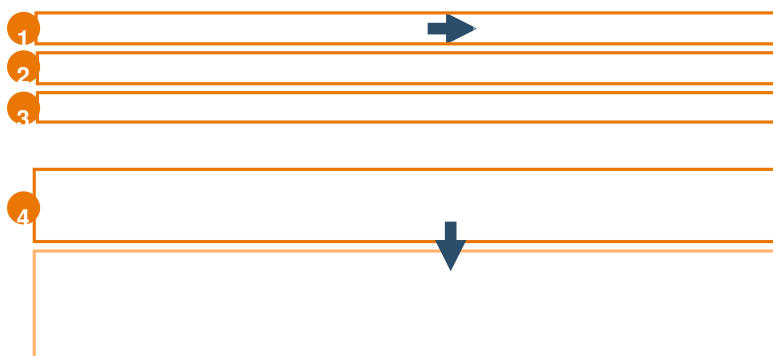
Подробнее о профилях аутентификации читайте в разделе руководства [Профили аутентификации](#).

Создание профиля безопасности VPN

В настройках профиля безопасности VPN определяются типы и параметры алгоритмов шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов.

Для создания профиля безопасности в веб-консоли администратора **VPN-сервера** необходимо перейти в раздел **VPN → Серверные профили безопасности**:

Нажать кнопку **Добавить** в панели инструментов раздела и заполнить необходимые поля в свойствах профиля безопасности:



Вкладка **Общие** предназначена для выбора версии протоколов VPN и задания параметров аутентификации при установлении защищенного соединения.

1. **Протокол.** Возможны следующие варианты выбора поля:

- **IPsec/L2TP.**
- **IKEv2.**
- **IPsec only/IKEv1** — не используется для организации соединений Remote access VPN (используется только для организации соединений Site-to-Site VPN).

2. **Режим работы IKE** (доступно только для IKEv1) (Подробнее о режимах IKEv1 читайте в статье [VPN](#)). Возможны следующие варианты выбора поля:

- **Основной.**
- **Агрессивный.**

3. **Тип идентификации** (параметр IKE local ID). Необходим для идентификации DCFW на соседнем узле при установлении VPN-соединения с оборудованием некоторых производителей. Возможные значения выбора поля:

- **Отсутствует** — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID.
- **IPv4** — IP-адрес узла.
- **FQDN** — адрес узла в формате полностью определенного доменного имени (FQDN).
- **CIDR** — адрес узла в формате бесклассовой адресации (CIDR).
- **Значение идентификации** — значение параметра IKE local ID в формате выбранного ранее типа.

4. Тип аутентификация удаленного узла при установлении защищенного соединения.

- При выборе протоколов IPsec/L2TP используется аутентификация с **общим ключом** (Pre-shared key). Необходимо задать общий ключ. Строка должна совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
- При выборе протокола IKEv2 для организации туннеля указывается:
 - Заранее созданный **сертификат сервера**;
 - **Режим аутентификации** — возможна аутентификация с помощью сертификатов, использующих инфраструктуру открытых ключей (**PKI**), или с помощью протокола EAP с методом MSCHAPv2 (**AAA**).
 - При выборе режима **PKI** необходимо указать сконфигурированный ранее **профиль клиентского сертификата** (подробнее о профилях клиентских сертификатов смотрите в разделе [Профили клиентских сертификатов](#)).

- В режиме аутентификации с помощью протокола EAP с методом MSCHAPv2 (**AAA**) 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.

Далее необходимо задать криптографические параметры первой и второй фаз согласования защищенного соединения.

Во время первой фазы происходит согласование и установление IKE SA. Необходимо указать следующие параметры:

5

6

7

8

5. **Время жизни ключа** — по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.

6. Режим работы механизма **Dead peer detection** (DPD) — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны 3 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 есть, 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, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова 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.

7. **Diffie-Hellman группы** — выбор групп Диффи-Хеллмана, которые будет использоваться для обмена ключами.

8. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Во второй фазе осуществляется выбор способа защиты передаваемых данных в IPsec подключении. Необходимо указать следующие параметры:

9

10

11

12

9. **Время жизни ключа** — по истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.

10. **Максимальный размер данных, шифруемых одним ключом** — время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии.

11. **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 реер-узла для поддержания сессии NAT активной.

12. **Безопасность** — алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Для примера в веб-консоли администратора создан профиль безопасности **Remote Access VPN profile**, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, необходимо изменить общий ключ шифрования при использовании протоколов IKEv1/IPsec.

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

VPN-интерфейс в веб-консоли администратора создается в разделе **Сеть → Интерфейсы**. Необходимо нажать кнопку **Добавить** и выбрать **Добавить VPN**, далее в настройках VPN-адаптера задать необходимые параметры:

1. **Включено** — включение/отключение интерфейса.

2. **Название** — название интерфейса, должно быть в виде *tunnelN*, где *N* — это порядковый номер VPN-интерфейса.

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к DCFW, будут также помещены в эту зону. В этом поле указывается зона, созданная ранее на этапе [создания зоны для VPN подключений](#).

4. **Профиль netflow**, используемый для данного интерфейса. Подробнее о профилях netflow читайте в статье [Профили netflow](#). Опциональный параметр.

5. **Алиас/Псевдоним** интерфейса. Опциональный параметр.

6. **Режим** — тип присвоения IP-адреса. Возможные опции выбора — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Remote access VPN), то необходимо использовать статический IP-адрес.

7. **MTU** — размер MTU для выбранного интерфейса. Если пакеты, передаваемые через VPN-туннель, превышают максимальный размер MTU

на любом из промежуточных устройств, они могут быть разделены на фрагменты. Это может привести к увеличению задержки и потере производительности. Путем установки оптимального значения MTU на туннельном интерфейсе можно избежать фрагментации и снизить задержку.

8. Поле добавления **IP-адреса** VPN-интерфейса в случае, если выбран статический режим присвоения адреса.

Для примера в веб-консоли администратора создан VPN-интерфейс **tunnel1**, который может быть использован для Remote Access VPN.

Создание сети VPN

Сеть VPN определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов.

Сеть VPN в веб-консоли администратора создается в разделе **VPN → Сети VPN**, Необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах VPN-сети:

1. **Название** сети VPN.

2. **Описание** сети VPN. Опциональный параметр.

3. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен **VPN-интерфейсу** DCFW, используемому совместно с данной сетью. Не указывайте здесь адрес сети и широковещательный адрес.

4. **Маска** сети VPN.

5. Указать **DNS-серверы**, которые будут переданы клиенту, или поставить флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует DCFW.

Важно! Можно указать не более двух DNS-серверов.



6. **Маршруты VPN** — маршруты, передаваемые VPN-клиенту в виде бесклассовой адресации (CIDR) или заранее созданного списка IP-адресов.



7. Вкладка **Маршруты для UserGate client** предназначена для настройки функциональности раздельного туннелирования (split tunneling) для UserGate Client.

Для примера в веб-консоли администратора создана сеть **Remote access VPN network** с настройками по умолчанию. Для использования этой сети в ней необходимо добавить маршруты, передаваемые на клиент.

Создание серверного правила VPN

Серверные правила VPN в веб-консоли администратора создаются в разделе **VPN → Серверные правила**. Далее необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах правила:

1

2

3

4

5

6

7

8

1. **Включено** — включение/отключение правила VPN.
2. **Название** серверного правила VPN.
3. **Описание** серверного правила VPN. Опциональный параметр.
4. **Профиль безопасности VPN** — профиль безопасности, [созданный ранее](#).
5. **Сеть VPN** — сеть, созданная ранее на этапе [создания сети VPN](#).
6. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, [созданный ранее](#).
7. **Интерфейс** — созданный ранее [VPN-интерфейс](#).
8. **Только для UserGate Client** — опция (доступна начиная с релиза ПО 7.1.2) позволяет ограничить возможность подключения по данному правилу только для VPN-клиентов UserGate Client.

9

9. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**.

Важно! Обработка трафика происходит по следующей логике:

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



10. **Пользователи** — локальные или доменные группы учетных записей пользователей или отдельные учетные записи пользователей, которым разрешено подключаться по VPN.



11 **Назначение** — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на этапе [контроля доступа зоны](#).

Важно! Для применения различных серверных правил к разным клиентам необходимо использовать параметры [Зона источника](#) и [Адрес источника](#). Параметр [Пользователи](#) не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.

Примечание При изменении настроек VPN-сервера (изменение серверных правил, изменение профилей безопасности, добавление новых VPN-сетей) не происходит перезагрузка VPN-сервера, благодаря чему ранее установленные активные сессии VPN-клиентов не обрываются. Перезагрузка VPN-сервера и переподключение активных сессий VPN-клиентов может произойти в случае смены IP-адреса туннельного интерфейса VPN-сервера.

Для примера в веб-консоли администратора создана сеть **Remote access VPN network** с настройками по умолчанию. Для использования этой сети в ней необходимо добавить маршруты, передаваемые на клиент.

Контроль доступа к ресурсам

Клиенты подключаются к VPN с использованием Point-to-Point протокола. Чтобы трафик мог ходить из созданной ранее [зоны для VPN-подключений](#), необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT** и

маршрутизация. Подробнее о правилах NAT читайте в разделе [NAT и маршрутизация](#). Для примера в веб-консоли администратора 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, или, например, для предоставления доступа в интернет в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из [зон для VPN-подключений](#) в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в разделе руководства [Межсетевой экран](#).

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило отключено по умолчанию.

Настройка VPN-клиента

После настройки VPN-сервера необходимо настроить VPN-клиенты. В качестве клиентского ПО на устройствах пользователей может использоваться UserGate Client, также поддерживаются нативные клиенты большинства популярных операционных систем.

Настройка параметров клиентского ПО зависит от типа устанавливаемого соединения.

L2TP/IPsec VPN

При создании VPN с помощью L2TP/IPsec(IKEv1), протокол L2TP создает туннель, в котором передаются пакеты сетевого уровня в кадрах PPP. IPsec обеспечивает шифрование, аутентификацию и проверку целостности передаваемых данных.

Взаимная аутентификация узлов осуществляется посредством **общего ключа** (Pre-shared key). Аутентификация пользователей VPN производится с помощью логина и пароля.

В настройках клиентского ПО необходимо указать следующие параметры:

- Тип VPN (L2TP/IPsec);
- Имя или IP-адрес VPN-сервера;
- Значение общего ключа (pre-shared key);
- Метод аутентификации пользователя (PAP);
- Параметры первой и второй фаз согласования защищенного соединения;
- Параметры аутентификации пользователя (логин и пароль).

Операционные системы Windows версий 10 и выше, по умолчанию, не поддерживают L2TP-подключения к серверам, которые находятся за вышестоящими маршрутизаторами с функционалом NAT. Для возможности установки соединения необходимо внести следующие правки в реестр ОС Windows:

- в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent** создать параметр **DWORD (32 бита)** с названием **AssumeUDPEncapsulationContextOnSendRule** и значением **2**;
- в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters** изменить значение параметра **AllowL2TPWeakCrypto** на **1**.

Важно! После внесения изменений в реестр их необходимо применить, например, перезагрузив компьютер.

Для получения более подробной информации обратитесь к статье Microsoft (<https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/configure-l2tp-ipsec-server-behind-nat-t-device>).

IPsec (IKEv2) VPN с аутентификацией посредством сертификатов, использующих инфраструктуру открытых ключей (PKI)

При создании VPN с помощью IPsec(IKEv2) защищенный VPN-туннель создается только протоколами группы IPsec с протоколом IKE версии 2 (IKEv2). В процессе создания туннеля происходит взаимная аутентификация узлов с проверкой подлинности сертификатов.

Проверка сертификатов происходит следующим образом:

- По зашифрованному каналу VPN-клиент присылает свой сертификат и зашифрованные данные, подписанные приватным ключом.
- VPN-сервер расшифровывает данные публичным ключом клиента и сравнивает со своим контрольным набором, тем самым проверяется наличие приватного ключа у клиента.
- VPN-сервер проверяет сертификат клиента на соответствие указанной цепочки сертификатов, тем самым проверяется, что сертификат выписан от имени уполномоченного УЦ.
- VPN-сервер может проверить сертификат на отозванность.
- VPN-сервер извлекает имя пользователя из сертификата и ищет пользователя с использованием метода, указанного в настроенном профиле аутентификации.
- Если не пройдет любой из указанных пунктов проверки, соединение не установится.
- Если все проверки пройдены, VPN-сервер со своей стороны отправляет свой сертификат и зашифрованные данные, подписанные своим приватным ключом.
- VPN-клиент проверяет правильность подписи сервера и соответствие имени сервера из сертификата тому адресу, куда он подключился.

При настройке клиентского ПО необходимо выполнить следующие операции:

- Импортировать заранее созданный клиентский сертификат и сертификат корневого центра на рабочую станцию;
- Указать тип VPN (IKEv2);
- Указать адрес VPN-сервера;
- Указать метод аутентификации;
- Выполнить настройки параметров виртуального адаптера.

IPsec (IKEv2) VPN с аутентификацией с помощью протокола EAP с методом MSCHAPv2 (AAA)

При создании VPN с помощью IPsec (IKEv2) защищенный VPN-туннель создается только протоколами группы IPsec с протоколом IKE версии 2 (IKEv2).

В режиме аутентификации с помощью протокола EAP MSCHAPv2 (AAA) во время фазы обмена IKE_AUTH VPN-сервер отвечает клиенту, что требуется авторизация через EAP. Клиент обменивается с VPN-сервером несколькими 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 и принадлежности его к тем или иным группам, после чего принимает решение о подключении пользователя к VPN. Также в процессе установления соединения VPN-клиент производит проверку подлинности сертификата VPN-сервера.

При настройке клиентского ПО необходимо выполнить следующие операции:

- Импортировать сертификат корневого центра на рабочую станцию;
- Указать тип VPN (IKEv2);
- Указать адрес VPN-сервера;
- Указать метод аутентификации;
- Указать параметры аутентификации пользователя (логин и пароль);
- Выполнить настройки параметров виртуального адаптера.

