

Table of Contents

Table of Contents	1
Настройка VPN	2
Описание	3
VPN для защищенного соединения офисов (Site-to-Site VPN)	4
VPN для удаленного доступа клиентов (Remote access VPN)	10
IPsec over GRE	14
GRE over IPsec	15

Описание

Documentation: 

Version: 5.x, 6.1.9, 7.0.1

VPN ([Virtual Private Network](#) — виртуальная частная сеть) — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, [интернет](#)). NGFW позволяет создавать VPN-подключения следующих типов:

- VPN-сервер для удаленного доступа клиентов (**Remote access VPN**). В данном случае NGFW выступает в качестве сервера, а пользователи других устройств выступают в качестве клиентов VPN. NGFW поддерживает работу со стандартными клиентами большинства популярных операционных систем, например, таких, как Windows, Linux, Mac OS X, iOS, Android и другие.
- VPN для защищенного соединения офисов (Site-to-Site VPN). В данном случае один NGFW выступает в качестве сервера, а другой NGFW выступает в роли клиента. Клиент инициирует соединение с сервером. Подключение сервер-сервер позволяет объединить разобщенные офисы компании в единую логическую сеть.

Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec. Поддерживается многофакторная аутентификация пользователей при подключении к сервису VPN.

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

Product: UserGate NGFW

Version: 6.1.9, 7.0.1

Technology: VPN

Хотя настройка NGFW для выполнения роли VPN-сервера близка к настройке сервера для удаленного доступа, мы рекомендуем произвести все настройки отдельно, поскольку часть настроек может отличаться.

Настройка сервера, выполняющего роль VPN-сервера для объединения офисов:

Наименование	Описание
Шаг 1. Создать локального пользователя для авторизации сервера, выступающего в роли VPN-клиента.	В разделе Пользователи и устройства → Пользователи создать пользователей для каждого из удаленных NGFW, выступающих в роли VPN-клиентов, задать пароли. Рекомендуется поместить всех созданных пользователей в группу, которой будет дан доступ для подключения по VPN. По умолчанию для этой цели в NGFW создана группа VPN servers .
Шаг 2. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.	В разделе Сеть → Зоны отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервис VPN. Как правило, это зона Untrusted .
Шаг 3. Создать зону, в которую будут помещены подключаемые по VPN серверы.	В разделе Сеть → Зоны создать зону, в которую будут помещены подключаемые по VPN серверы. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Рекомендуется использовать уже существующую по умолчанию зону VPN for Site-to-Site .
Шаг 4. Создать разрешающее правило межсетевого экрана для трафика из созданной зоны.	В разделе Политики сети → Межсетевой экран создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны. По умолчанию в NGFW создано правило межсетевого экрана VPN for Site-to-Site to Trusted and Untrusted , разрешающее весь трафик из зоны VPN for Site-to-Site в Trusted и Untrusted зоны. Правило выключено по умолчанию. Чтобы трафик передавался клиенту из нужной зоны сервера через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения VPN for Site-to-Site .
Шаг 5. Создать профиль авторизации.	В разделе Пользователи и устройства → Профили авторизации создать профиль авторизации для пользователей VPN. Допускается использовать тот же профиль авторизации, что используется для авторизации пользователей с целью получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной авторизации, такие как Kerberos, NTLM, SAML IDP. Подробнее о профилях авторизации смотрите в разделе данного руководства Профили авторизации.

Наименование	Описание
Шаг 6. Создать профиль безопасности VPN.	Профиль безопасности определяет такие настройки, как общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов. Для создания профиля безопасности необходимо перейти в раздел VPN → Профили безопасности, нажать кнопку Добавить и заполнить следующие поля: • Название — название профиля безопасности. • Описание — описание профиля. • Версия протокола IKE (Internet Key Exchange). Протокол IKE используется для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1. • Режим IKE: Основной или Агрессивный. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. • Основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (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. • Агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 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. • Аутентификация с пиром. Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key). • Общий ключ — строка, которая должна совпадать на сервере и клиенте для успешного подключения. Далее необходимо задать параметры первой и второй фаз согласования. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • Интервал проверки dead peer detection — для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал: 10 секунд; значение 0 отключает проверку. • Неудачных попыток — максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • Diffie-Hellman группы: выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх/вниз или используйте кнопки Выше/Ниже. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • 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. • 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. • Алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх/вниз или используйте кнопки Выше/Ниже. По умолчанию в NGFW создан профиль безопасности Site-to-Site VPN profile, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, необходимо изменить общий ключ шифрования.

Наименование	Описание
Шаг 7. Создать VPN-интерфейс.	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 NGFW, 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. Внимание! Редактирование кластерного интерфейса возможно только для узла кластера cluster (даже если кластер не собран и узел всего один). В разделе Сеть → Интерфейсы нажмите кнопку Добавить и выберите Добавить VPN. Задайте следующие параметры: • Название — название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • Описание — описание интерфейса. • Зона — зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 3. • Профиль Netflow — профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • Режим — тип присвоения IP-адреса — 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. • MTU — размер MTU для выбранного интерфейса. По умолчанию в системе уже создан VPN-интерфейс tunnel2, который рекомендовано использовать для Site-to-Site VPN.
Шаг 8. Создать сеть VPN.	VPN-сеть определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и — опционально — маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов. Важно! Добавление сетей VPN лучше делать в технологическое окно, так как при добавлении новой сети VPN происходит рестарт сервиса из-за чего текущие VPN соединения прерываются на несколько десятков секунд. Для создания туннеля VPN перейдите в раздел VPN → Сети VPN, нажмите кнопку Добавить и заполните следующие поля: • Название — название сети. • Описание — описание сети. • Диапазон IP-адресов, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес. • Укажите DNS-серверы, которые будут переданы клиенту, или отметьте чекбокс Использовать системные DNS, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW. Важно! Можно указать не более двух DNS-серверов. • Укажите маршруты, передаваемые клиенту в виде бесклассовой адресации (CIDR). В NGFW создана сеть Site-to-Site VPN network с настройками по умолчанию. Для использования этой сети в ней необходимо добавить маршруты, передаваемые на сервер-клиент. Чтобы VPN-сервер узнал о подсетях клиента, необходимо прописать статический маршрут на сервере, указав в качестве адреса назначения адрес VPN-туннеля, используемый на сервере-клиенте.

Наименование	Описание
Шаг 9. Создать серверное правило VPN.	Создать серверное правило VPN, используя в нем созданные ранее сеть и профиль VPN. Для создания правила необходимо перейти в раздел VPN → Серверные правила, нажать кнопку Добавить и заполнить следующие поля: • Название — название правила. • Описание — описание правила. • Профиль безопасности — профиль безопасности VPN, созданный ранее. • Сеть VPN — сеть VPN, созданная ранее. • Профиль авторизации — профиль авторизации, созданный ранее. • 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. • Назначение — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на шаге 2. • Интерфейс — созданный ранее интерфейс VPN. • Пользователи — группа учетных записей серверов или отдельные учетные записи серверов, которым разрешено подключаться по VPN. По умолчанию в NGFW создано серверное правило Site-to-Site VPN rule, в котором используются необходимые настройки для Site-to-Site VPN, а доступ к VPN разрешен членам локальной группе VPN servers. Важно! Для применения различных серверных правил к разным клиентам необходимо использовать параметры <u>Исходная зона</u> и <u>Адрес источника</u>. Параметр <u>Пользователь</u> не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.

Для настройки сервера, выступающего в роли VPN-клиента, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону, в которую будут помещены интерфейсы, используемый для подключения по VPN.	В разделе Сеть → Зоны создать зону, в которую будут помещены интерфейсы, используемые для подключения по VPN. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Рекомендуется использовать уже существующую по умолчанию зону VPN for Site-to-Site.
Шаг 2. Создать разрешающее правило межсетевого экрана для трафика в созданную зону.	Создать разрешающее правило межсетевого экрана в разделе Политики сети → Межсетевой экран. По умолчанию в NGFW создано правило межсетевого экрана VPN for Site-to-Site to Trusted and Untrusted, разрешающее весь трафик между зонами VPN for Site-to-Site, Trusted и Untrusted. 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 VPN for Site-to-Site.

Наименование	Описание
Шаг 3. Создать профиль безопасности VPN.	Профиль безопасности определяет такие настройки, как общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов. Для создания профиля необходимо перейти в раздел VPN → Профили безопасности VPN, нажать кнопку Добавить и заполнить следующие поля: • Название — название профиля безопасности. • Описание — описание профиля. • Версия протокола IKE (Internet Key Exchange). Протокол IKE используется для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1. • Режим IKE: Основной или Агрессивный. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. ◦ Основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (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. ◦ Агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 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. • Аутентификация с пиром. Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key). • Общий ключ — строка, которая должна совпадать на сервере и клиенте для успешного подключения. Далее необходимо задать параметры первой и второй фаз согласования. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • Интервал проверки dead peer detection — для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал: 10 секунд; значение 0 отключает проверку. • Неудачных попыток — максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • Diffie-Hellman группы: выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки Выше/Ниже. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • 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. • 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 достигший лимита, запустит пересоздание ключей сессии. • Алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки Выше/Ниже. По умолчанию в NGFW создан профиль Client VPN profile, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, то необходимо изменить общий ключ шифрования.

Наименование	Описание
Шаг 4. Создать VPN-интерфейс.	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 NGFW, 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. В разделе Сеть → Интерфейсы нажмите кнопку Добавить и выберите Добавить VPN. Задайте следующие параметры: • Название — название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • Описание — описание интерфейса. • Зона — зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 1. • Профиль Netflow — профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • Режим — тип присвоения IP-адреса — 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. • MTU — размер MTU для выбранного интерфейса. По умолчанию в системе уже создан VPN-интерфейс tunnel3, который рекомендовано использовать для клиентского подключения Site-to-Site VPN. Важно! Если при настройке туннельного интерфейса на стороне сервера был выбран уже существующий интерфейс tunnel2 с настройками по умолчанию, то на клиенте при подключении к серверу возникнет конфликт IP-адресов, поскольку на клиенте также существует аналогичный интерфейс tunnel2 с тем же диапазоном адресов. Для корректной работы диапазоны адресов туннельных интерфейсов не должны пересекаться. Рекомендуется изменить диапазон адресов на клиенте на уникальный.
Шаг 5. Создать клиентское правило VPN.	Создать клиентское правило VPN, которое будет инициировать подключение к VPN-серверу. Для создания правила необходимо перейти в раздел VPN → Клиентские правила, нажать кнопку Добавить и заполнить следующие поля: • Включено — включение/отключение данного правила. • Название — название правила. • Описание — описание правила. • Профиль безопасности VPN — созданный ранее профиль безопасности VPN. • Интерфейс — созданный ранее VPN-интерфейс. • Адрес сервера — IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне Untrusted на NGFW, выполняющего роль VPN-сервера. • Протокол VPN — Возможно выбрать вариант L2TP/IPsec или IPsec туннель для подключения к VPN-серверу. • Подсети для VPN — IP адрес сети, которая будет доступна для клиентов со стороны NGFW и со стороны VPN-сервера. • Имя пользователя и пароль (только для протокола L2TP) — имя и пароль пользователя, созданного на шаге 1 при подготовке VPN-сервера.

Примечание В сценарии site-to-site VPN-подключение по протоколам L2TP/IPsec полностью поддерживается между устройствами UserGate. Клиентское подключение UserGate NGFW к VPN-серверам сторонних производителей по протоколам L2TP/IPsec не поддерживается. При работе UserGate NGFW в режиме VPN-сервера L2TP/IPsec передача маршрутов выполняется через payload L2TP.

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

VPN для удаленного доступа клиентов (Remote access VPN)

Documentation: ☒
Version: 6.1.9, 7.0.1

Для подключения VPN-клиентов к корпоративной сети необходимо настроить NGFW для выполнения роли VPN-сервера. Для этого необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.	В разделе Сеть → Зоны отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервис VPN. Как правило, это зона Untrusted .
Шаг 2. Создать зону, в которую будут помещены подключаемые по VPN клиенты.	В разделе Сеть → Зоны создать зону, в которую будут помещены подключаемые по VPN клиенты. Эту зону в дальнейшем можно использовать в политиках безопасности. Рекомендуется использовать уже существующую по умолчанию зону VPN for remote access .
Шаг 3. Создать правило NAT для созданной зоны.	Клиенты подключаются к VPN с использованием Point-to-Point протокола. Чтобы трафик мог ходить из созданной на предыдущем шаге зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Создайте соответствующее правило в разделе Политики сети → NAT и маршрутизация . По умолчанию в NGFW создано правило NAT from VPN for remote access to Trusted and Untrusted , разрешающее подмену адресов из зоны VPN for remote access в зоны Trusted и Untrusted .
Шаг 4. Создать разрешающее правило межсетевого экрана для трафика из созданной зоны.	В разделе Политики сети → Межсетевой экран создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны. По умолчанию в 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 .
Шаг 5. Создать профиль аутентификации.	В разделе Пользователи и устройства → Профили аутентификации создать профиль авторизации для пользователей VPN. Допускается использовать тот же профиль авторизации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной авторизации, такие как Kerberos, NTLM, SAML IDP. VPN поддерживает многофакторную аутентификацию. Второй фактор может быть получен через одноразовые коды ТOTP. Для ввода второго фактора аутентификации пользователь при подключении к VPN серверу должен указать свой пароль в виде: пароль:одноразовый_код где пароль — это пароль пользователя : — разделитель одноразовый_код — второй фактор аутентификации. Подробнее о профилях авторизации смотрите в разделе данного руководства Профили аутентификации . Внимание! В версиях NGFW старше 6.1.8 данный раздел носит название Профили авторизации

Наименование	Описание
Шаг 6. Создать профиль безопасности VPN.	Профиль безопасности VPN определяет такие настройки, как общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей и использовать их для построения соединений с разными типами клиентов. Для создания профиля необходимо перейти в раздел VPN → Профили безопасности VPN, нажать кнопку Добавить и заполнить следующие поля: • Название — название профиля безопасности. • Описание — описание профиля. • Версия протокола IKE (Internet Key Exchange). Протокол IKE используется для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1. • Режим IKE: Основной или Агрессивный. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. • Основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (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. • Агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 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. • Аутентификация с пиром. Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key). • Общий ключ — строка, которая должна совпадать на сервере и клиенте для успешного подключения. Далее необходимо задать параметры первой и второй фаз согласования. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • Интервал проверки dead peer detection — для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал проверки: 10 секунд; значение 0 отключает проверку. • Неудачных попыток — максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • Diffie-Hellman группы: выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки Выше/Ниже. Важно При работе с операционными системами Windows и Android необходимо отключать проверку dead peer detection. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • 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. • 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. • Алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки Выше/Ниже. По умолчанию в NGFW создан серверный профиль Remote access VPN profile, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, то необходимо изменить общий ключ шифрования. Для упрощения настройки соединения с устройствами других вендоров по умолчанию созданы дополнительные профили безопасности (Cisco compatible VPN profile — для работы с устройствами Cisco и Fortinet compatible VPN profile — для работы с устройствами Fortinet).

Наименование	Описание
Шаг 7. Создать VPN-интерфейс.	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 NGFW, 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. В разделе Сеть → Интерфейсы нажмите кнопку Добавить и выберите Добавить VPN. Задайте следующие параметры: • Название — название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • Описание — описание интерфейса. • Зона — зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 2. • Профиль Netflow — профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • Режим — тип присвоения IP-адреса — 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. • MTU — размер MTU для выбранного интерфейса. По умолчанию в системе уже создан VPN-интерфейс tunnel1, который рекомендовано использовать для Remote access VPN.
Шаг 8. Создать сеть VPN.	VPN-сеть определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и — опционально — маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов. Важно! Добавление сетей VPN лучше делать в технологическое окно, так как при добавлении новой сети VPN происходит рестарт сервиса из-за чего текущие VPN соединения прерываются на несколько десятков секунд. Для создания туннеля VPN перейдите в раздел VPN → Сети VPN, нажмите кнопку Добавить и заполните следующие поля: • Название — название сети. • Описание — описание сети. • Диапазон IP-адресов, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес. • Укажите DNS-серверы, которые будут переданы клиенту, или отметьте чекбокс Использовать системные DNS, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW. Важно! Можно указать не более двух DNS-серверов. • Укажите маршруты, передаваемые клиенту в виде бесклассовой адресации (CIDR). В NGFW создана сеть Remote access VPN network с рекомендуемыми настройками.

Наименование	Описание
Шаг 9. Создать серверное правило VPN.	Создать серверное правило VPN, используя в нем созданные ранее сеть VPN, интерфейс VPN и профиль VPN. Для создания правила необходимо перейти в раздел VPN → Серверные правила, нажать кнопку Добавить и заполнить следующие поля: • Включено — включает/отключает правило. • Название — название правила. • Описание — описание правила. • Профиль безопасности — профиль безопасности, созданный ранее. • Сеть VPN — сеть VPN, созданная ранее. • Профиль авторизации — профиль авторизации, созданный ранее. • URL инициализации TOTP — url, по которому пользователь может провести первоначальную инициализацию своего TOTP-устройства в случае, если настроена многофакторная авторизация TOTP для авторизации VPN. • Интерфейс — интерфейс VPN, созданный ранее. • 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. • Назначение — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на шаге 1. • Пользователи — группа пользователей или отдельные пользователи, которым разрешено подключаться по VPN. По умолчанию в NGFW создано серверное правило Remote access VPN rule, в котором используются необходимые настройки для Remote Access VPN, а доступ к VPN разрешен членам локальной группы VPN users. Важно! Для применения различных серверных правил к разным клиентам необходимо использовать параметры <i>Исходная зона</i> и <i>Адрес источника</i>. Параметр <i>Пользователь</i> не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.
Шаг 10. Настроить VPN на клиентском компьютере.	Для настройки клиентского подключения к VPN на компьютере пользователя необходимо указать следующие параметры: • Используйте тип подключения VPN — L2TP over IPsec. • В качестве IP-адреса VPN-сервера укажите IP-адрес интерфейса зоны, указанной на шаге 1. • В качестве общего ключа (pre-shared key, shared secret) используйте общий ключ, указанный вами на шаге 6. • Укажите протокол PAP для авторизации пользователя. • В качестве имени пользователя укажите имя учетной записи пользователя в формате username @domain, например, testuser@testdomain.loc • В настройках VPN-подключения отключите использование основного шлюза в удаленной сети. Важно! Операционные системы Microsoft Windows требуют изменения параметров реестра для корректной работы с VPN-сервером L2TP/IPsec. 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 over GRE

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1, 6.1.9

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.

Для настройки IPsec over GRE необходимо:

Наименование	Описание
Шаг 1. 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 внешние IP-адреса интерфейсов устройства.
Шаг 2. Настройка Site-to-Site VPN-соединения.	Подробнее о настройке Site-to-Site VPN-соединения читайте в разделе VPN для защищенного соединения офисов (Site-to-Site VPN) . Важно! При настройке клиентского правила VPN в качестве адреса сервера необходимо указать IP-адрес туннельного интерфейса GRE.

Недостаток IPsec over GRE: не поддерживается передача многоадресных и широковещательных пакетов. Эта проблема отсутствует при использовании соединения GRE over IPsec.

GRE over IPsec

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1, 6.1.9

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 в GRE пакеты, а затем их передача по зашифрованному каналу связи (инкапсуляция IPsec).

Для настройки GRE over IPsec необходимо:

Наименование	Описание
Шаг 1. Настройка Site-to-Site VPN-соединения.	Подробнее о настройке Site-to-Site VPN-соединения читайте 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.

