

Table of Contents

Table of Contents	1
Глобальный портал	2
Общие сведения	3
Веб-портал (SSL VPN)	4
Публикация ресурсов с помощью reverse-прокси	7

Общие сведения

Documentation: ☒

Product: NGFW

Version: 7.x

Веб-портал и reverse-прокси, наряду с правилами DNAT/Порт-форвардинга, позволяют опубликовать ресурсы, находящиеся внутри компании, пользователям из интернета.

При наличии публикаций внутренних ресурсов с помощью DNAT/Порт-форвардинга, reverse-прокси и веб-портала порядок обработки правил следующий:

1. Правила DNAT/Порт-форвардинга.
2. Правила веб-портала. Если имя хоста в запросе совпало с именем хоста веб-портала, и номер порта в запросе совпал с номером порта, указанного для работы веб-портала, то отработывают правила веб-портала.
3. Правила Reverse-прокси.

Documentation: 
Product: NGFW
Version: 7.x

Веб-портал позволяет предоставить доступ к внутренним веб-ресурсам, терминальным и ssh-серверам компании для удаленных или мобильных пользователей, используя при этом только протокол HTTPS. Данная технология не требует установки специального клиента VPN, достаточно обычного браузера.

ПримечаниеЕсли на целевых HTTP-ресурсах настроена аутентификация Kerberos или NTLM, то NGFW может производить аутентификацию по технологии SSO (необходим настроенный LDAP-коннектор с загруженным keytab-файлом). При этом аутентификация на самом NGFW также должна быть настроена через Kerberos/NTLM, так как NGFW передаёт данные прозрачно, форма аутентификации при ответе сайта с ошибкой 401 (Unauthorized) не передается клиенту веб-портала.

ПримечаниеНачиная с версии 7.4.0 для создания защищенного соединения с веб-серверами UserGate NGFW использует алгоритмы шифрования GCM с повышенной устойчивостью к уязвимостям и атакам. Поэтому, перед тем как настроить передачу трафика по защищенному соединению, необходимо убедиться, что веб-сервер поддерживает алгоритмы шифрования GCM и согласует их в сообщениях «server hello» при установлении соединения.

Для настройки веб-портала необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Включить и настроить веб-портал.	В разделе Настройки → Веб-портал включить и настроить параметры веб-портала. Подробные значения настроек будут описаны далее в этой главе
Шаг 2. Разрешить доступ к сервису веб-портала на необходимых зонах.	В разделе Сеть → Зоны разрешить сервис веб-портала для выбранных зон (обычно зона Untrusted). Данное разрешение откроет доступ к порту сервиса, который был указан в настройках веб-портала на предыдущем шаге
Шаг 3. Добавить внутренние ресурсы в веб-портал.	В разделе Глобальный портал → Веб-портал добавить URL внутренних ресурсов, к которым необходим доступ пользователей. Подробные значения настроек будут описаны далее в этой главе

При настройке веб-портала (раздел **Настройки → Веб-портал**) необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает/Выключает веб-портал
Имя хоста	Имя хоста, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. Данное имя должно резолвиться службами DNS в IP-адрес интерфейса NGFW, входящего в зону, на которой разрешен сервис веб-портала
Порт	Порт TCP, который будет использоваться сервисом веб-портала. Порт вместе с именем хоста образуют URL для подключения пользователей в виде: https://имя_хоста:порт
Профиль аутентификации	Профиль аутентификации пользователей, который будет использоваться для аутентификации пользователей, подключающихся к веб-порталу. Профиль аутентификации задает метод аутентификации, например, AD-коннектор или локальный пользователь. Также в профиле аутентификации можно указать требование использовать мультифакторную аутентификацию для доступа к веб-порталу. Подробнее о профилях аутентификации — в разделе « Профили аутентификации »
Шаблон страницы аутентификации	Выбрать шаблон страницы аутентификации, который будет использоваться для отображения формы для ввода логина и пароля. Вы также можете создать свою страницу аутентификации. Подробнее об этом — в разделе « Шаблоны страниц »
Шаблон портала	Выбрать шаблон веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Вы также можете создать свой шаблон веб-. портала. Подробнее об этом — в разделе « Шаблоны страниц »

Наименование	Описание
Предлагать выбор домена AD/LDAP на странице аутентификации	Показывать выбор домена на странице аутентификации веб-портала.
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице аутентификации веб-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о профилях SSL — в разделе « Профили SSL »
Сертификат	Сертификат, который будет использоваться для создания HTTPS-соединения. Если выбран режим Автоматически , то используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Подробнее о ролях сертификатов — в разделе « Управление сертификатами »
Аутентификация пользователя по сертификату	Если выбрано, то требует предъявления пользовательского сертификата браузером. Для этого пользовательский сертификат должен быть добавлен в список сертификатов NGFW, ему должна быть назначена роль Пользовательский сертификат и назначен соответствующий пользователь NGFW. Подробнее о пользовательских сертификатах — в разделе « Управление сертификатами »

Настройка веб-портала (раздел **Глобальный портал** → **Веб портал**) сводится к тому, что необходимо создать записи публикации URL внутренних веб-ресурсов. Для каждого URL необходимо создать закладку и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает закладку
Название	Название закладки
Описание	Описание закладки
URL	URL ресурса, который необходимо опубликовать через веб-портал. Указывайте полный URL, начиная с http:// , https:// , ftp:// , ssh:// или rdp://. Важно! Для публикации терминальных серверов необходимо отключить опцию, требующую Network Level Authentication в свойствах RDP доступа на серверах терминального доступа. Аутентификацию пользователей для доступа к серверам в данном случае будет выполнять веб-портал в соответствии со своими настройками
Домен прямого доступа	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену. Домены прямого доступа должны быть локальными, и их разрешение должно происходить через DNS-сервер, установленный внутри локальной сети. При указании домена прямого доступа нужно выбрать профиль SSL. Выбор сертификата в этом случае не является обязательным. Если сертификат не выбран, он будет сгенерирован UG NGFW
Проверять авторизацию для RDP-сессий	Разрывать сессию RDP по завершению аутентификации на веб-портале на стороне сервера
Включить прозрачную аутентификацию	Прозрачная аутентификация позволяет аутентифицировать пользователя на опубликованном для него приложении. Для аутентификации будут использованы те же данные, что пользователь ввел при входе на веб-портал. Для успешной работы этой опции необходимо, чтобы опубликованное приложение поддерживало прозрачную аутентификацию
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о профилях SSL — в разделе « Профили SSL »
Сертификат	Сертификат, который будет использоваться для для создания HTTPS-соединения между NGFW и сервером. Если выбран режим Выбрать сертификат , то используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Подробнее о ролях сертификатов — в разделе « Управление сертификатами »

Наименование	Описание
Иконка	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из predetermined иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку
Вспомогательные URL	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Например, основной URL http://www.example.com получает часть медиаконтента со вспомогательного URL http://cdn.example.com
Пользователи	Список пользователей и/или групп пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL

Очередность закладок веб-портала определяет порядок отображения их пользователю. Администратор может менять очередность закладок с помощью кнопок **Выше/Ниже**, **Наверх/Вниз** или перетаскивая закладки с помощью мыши.

Documentation: 

Product: NGFW

Version: 7.x

UserGate NGFW поддерживает публикацию веб-серверов удаленных приложений в режиме сервера reverse-прокси. Доступ к веб-серверам и безопасность соединений с ними контролируются настраиваемыми правилами reverse-прокси.

Режим сервера reverse-прокси предоставляет следующие возможности:

- **Балансировка нагрузки.** Если обработку запросов к удаленному приложению выполняют несколько веб-серверов, сервер reverse-прокси может равномерно распределять запросы между ними и тем самым предотвращать перегрузку отдельных веб-серверов.
- **Переопределение URL-адресов.** Сервер reverse-прокси может выполнять подмену путей и доменных имен в запросах, чтобы перенаправить их на разные веб-серверы, помогая таким образом разделить трафик для разных приложений.
- **Управление доступом к веб-серверам.** Сервер reverse-прокси может блокировать попытки доступа по идентификационной строке клиентского приложения (useragent) и нежелательным адресам.
- **Поддержка SSL-подключения.** Сервер reverse-прокси может выполнять шифрование и расшифрование запросов и ответов, что позволяет снизить нагрузку на веб-серверы и повысить их производительность.

Чтобы опубликовать веб-сервер:

1. Создайте один или несколько серверов reverse-прокси.
2. Если для доступа к удаленному приложению развернуто несколько веб-серверов, создайте для них правило балансировки.
3. Создайте правила reverse-прокси, которые будут определять условия публикации веб-сервера или группы веб-серверов.

Важно! Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в параметрах правила.

4. В разделе **Настройки → Сеть → Зоны** в параметрах контроля доступа той зоны, в которой необходимо разрешить доступ к внутренним ресурсам, разрешите сервис **Reverse-прокси**.

Создание сервера reverse-прокси

Чтобы создать сервер reverse-прокси:

1. В разделе **Глобальный портал → Серверы reverse-прокси** нажмите **Добавить**.
2. В окне **Настройка сервера reverse-прокси** укажите название, IP-адрес или FQDN и TCP-порт публикуемого веб-сервера, .
3. Если необходимо, настройте остальные параметры:
 - Установите флажок **HTTPS до сервера**, чтобы выполнять передачу трафика по защищенному соединению от UserGate NGFW до публикуемого веб-сервера. Если этот флажок установлен, убедитесь, что на шаге 2 вы указали порт для защищенного соединения.

Примечание Начиная с версии 7.4.0 для создания защищенного соединения с веб-серверами UserGate NGFW использует алгоритмы шифрования GCM с повышенной устойчивостью к уязвимостям и атакам. Поэтому, перед тем как настроить передачу трафика по защищенному соединению, необходимо убедиться, что веб-сервер поддерживает алгоритмы шифрования GCM и согласует их в сообщениях «server hello» при установлении соединения.

- Установите флажок **Проверять SSL-сертификат**, чтобы включить проверку подлинности SSL-сертификата, установленного на публикуемом веб-сервере. Доступно, если установлен флажок **HTTPS до сервера**.
- Установите флажок **Не изменять IP-адрес источника**, чтобы сохранять оригинальный IP-адрес источника в запросах. Если флажок снят, IP-адрес источника заменяется на IP-адрес UserGate NGFW.

Важно! Если установлен флажок «Не изменять IP-адрес источника», для корректной работы необходимо настроить маршрутизацию таким образом, чтобы веб-сервер отвечал через тот же сетевой интерфейс UG NGFW, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UG NGFW или можно настроить статические маршруты через UG NGFW для «белых» IP-адресов источников.

4. Сохраните изменения.

Балансировка серверов reverse-прокси

Если для доступа к удаленному приложению развернуто несколько веб-серверов, вы можете распределять клиентские запросы между ними с помощью правил балансировки нагрузки.

Чтобы создать правило балансировки серверов reverse-прокси:

1. В разделе **Глобальный портал** создайте серверы reverse-прокси для удаленного приложения. Убедитесь, что в окне **Настройка сервера reverse-прокси** для каждого сервера, который участвует в балансировке, в поле **Адрес сервера** указан IP-адрес.
2. В разделе **Настройки → Политики сети → Балансировка нагрузки** нажмите **Добавить** и выберите **Добавить балансировщик reverse-прокси**.

3. В окне **Настройка правила балансировки reverse-прокси** на вкладке **Общие** укажите название правила и включите его.
4. На вкладке **Серверы reverse-прокси** добавьте серверы, на которые будет распределяться нагрузка.
5. Сохраните изменения.

Создание правила публикации reverse-прокси

Правила публикации reverse-прокси позволяют фильтровать запросы к веб-серверам, контролировать доступ к ним и обеспечивать безопасное соединение.

Созданные правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нем условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете мышью перетаскивать правила в списке для изменения порядка применения правил.

Чтобы создать правило reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Правила reverse-прокси** нажмите **Добавить**.
2. В окне **Настройка правила reverse-прокси** на вкладке **Общие**:
 - Включите правило и укажите его название.
 - Если необходимо, укажите теги для маркировки правила. Подробнее — см. в разделе «[Теги](#)». Параметр доступен в версии ПО 7.3.0 и выше.
 - В списке **Сервер reverse-прокси** выберите сервер или балансировщик reverse-прокси, которому UserGate NGFW будет пересылать запросы.
 - Укажите порты, на которых UserGate NGFW будет слушать входящие запросы.
 - Установите флажок **Использовать HTTPS**, если необходимо, чтобы обмен трафиком с клиентом проходил по защищенному соединению.
 - Если флажок **Использовать HTTPS** установлен:
 - Выберите профиль SSL, поддерживающий нужные протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи.
 - Укажите сертификат веб-сервера для поддержки HTTPS-соединения.
 - Если необходимо, включите авторизацию пользователя по сертификату, выбрав значение **PKI**, и затем укажите предварительно созданный профиль клиентских сертификатов. Подробнее — см. в разделе «[Профили клиентских сертификатов](#)».
 - С помощью параметра **Вставить** настройте расположение правила в списке.

Примечание Параметр доступен, если в списке уже есть другие правила.

3. На вкладке **Источник** выберите минимум одну зону источника трафика, а также, если необходимо, добавьте списки IP-адресов, доменных имен или GeoIP-адреса (не более 15 адресов), для которых будет разрешен обмен трафиком с веб-серверами.

Важно! Не добавляйте в списки строки с символом «*», они будут игнорироваться.

Примечание Вы также можете настроить правило, игнорирующее источники трафика в указанных зонах и с выбранными адресами. Для этого на вкладке «Источник» нужно сформировать список нежелательных зон и/или адресов и в соответствующих блоках параметров включить «Инвертировать».

Примечание Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса.

Важно! Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменных имен; условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

4. Если на шаге 2 выбраны использование HTTPS и авторизация по клиентскому сертификату, на вкладке **Пользователи**, если необходимо, сформируйте список пользователей и групп, для которых будет применяться это правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Подробнее — см. в разделе «[Пользователи и группы](#)».

5. На вкладке **Назначение** укажите IP-адреса, назначенные на интерфейсы, которые принимают входящие соединения. Этот параметр следует настраивать, когда на один интерфейс UserGate NGFW назначено несколько IP-адресов либо несколько интерфейсов подключены к сети.

Примечание Вы также можете настроить правило, игнорирующее входящие соединения на указанные адреса. Для этого на вкладке «Назначение» укажите адреса и включите «Инвертировать».

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.

6. На вкладке **Useragent**, если необходимо, добавьте идентификационные строки клиентских браузеров, для которых будет разрешен обмен трафиком с веб-серверами.

Примечание Вы также можете настроить правило, игнорирующее определенные браузеры, запрашивающие доступ к веб-серверу. Для этого на вкладке «Useragent» нужно сформировать список нежелательных браузеров и включить «Инвертировать».

7. На вкладке **Подмена путей** настройте переопределение путей URL. Подробнее о подмене путей — в разделе ниже.

8. Сохраните изменения.

Подмена путей в правилах reverse-прокси

В этом разделе описан порядок работы функции подмены путей в правилах reverse-прокси для версии 7.2.0 и выше.

Подмена путей в правилах reverse-прокси используется для перенаправления HTTP-запроса пользователя на иной путь. Таким образом вы можете управлять разделением трафика для разных сервисов. Например, пользователь выполнил запрос на example.com/path1, а сервер reverse-прокси перенаправляет запрос на example.local/path2.

Чтобы настроить подмену путей в правиле reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Правила reverse-прокси** создайте или выберите правило.
2. В окне **Настройка правила reverse-прокси** на вкладке **Подмена путей** нажмите **Добавить** и заполните поля:
 - **Изменить с** — домен и/или путь URL, которые требуется изменить. Если в поле **Изменить с** указан домен, то правило reverse-прокси будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.
 - **Изменить на** — домен и/или путь URL, на которые требуется заменить старый.

Примечание Начиная с версии 7.5.0 вы можете настраивать подмену путей и для кириллических доменов.



3. Сохраните правило.

При обработке HTTP-запроса работает правило reverse-прокси, паттерн которого в поле **Изменить с** совпадет с путем URL в запросе. При срабатывании правила reverse-прокси происходит подмена пути в HTTP-запросе: паттерн из поля **Изменить с** меняется на паттерн из поля **Изменить на**. Если запрос пользователя не попадет ни под одно правило reverse-прокси, в ответ на него будет получена ошибка: 403 Forbidden.

Условия проверки соответствия

Синтаксис HTTP-запроса представляет собой следующую последовательность: <scheme>://<host>:<port>/<path>.

Паттерн в поле **Изменить с** состоит из последовательности <host>/<path> и должен удовлетворять следующим условиям:

- <host> — обязательный параметр. Совпадение строгое, наличие и отсутствие символа «/» в конце названия узла без пути равнозначно. Все названия узлов приводятся к нижнему регистру.
- <path> — необязательный параметр. Без него будет выбираться любой путь. Совпадение префиксное (не строгое).
- Паттерн из поля **Изменить с** и паттерн из поля **Изменить на** должны оба либо заканчиваться символом «/», либо не содержать его в конце. В противном случае подмена путей сработает некорректно.
- Схема (<scheme>) запроса игнорируется и не изменяется.
- Порт (<port>) запроса игнорируется и не изменяется.

При совпадении запроса и исходного паттерна правило считается сработавшим.

В таблице ниже приведены примеры срабатываний паттернов.

Исходный паттерн в правиле reverse-прокси	Примеры запросов, на которые правило работает	Примеры запросов, на которые правило не работает
test.dev	- test.dev - test.dev/ - test.dev/* - http://test.dev - test.dev:<любой порт>	- abc.com - test.develop - test.dev.lol
tesT.deV	- test.deV - tesT.deV/ - TEST.dev	- abc.com - test.develop - test.dev.lol
test.dev/co	- test.dev/co* - http://test.dev/co* - test.dev:<любой порт>/co*	- test.dev.lol/co* - test.dev/kool*
http://test.dev	- http://test.dev - http://test.dev/* - http://test.dev:<любой порт> - http://test.dev:<любой порт>/ - http://test.dev:<любой порт>/*	http://test.develop
http://test.dev/co	- http://test.dev/co* - http://test.dev:<любой порт>/co	http://test.dev/cool*

Правила подмены путей

Рассмотрим детальнее логику работы подмены путей.

Для этого создадим правило test.dev/exa → test.dev/ad/test и сделаем несколько запросов.

1) Запрос на [test.dev/exalala](#).

Параметр path = [/exalala](#). Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается [/exa](#). Оставшаяся часть: [lala](#).

При дальнейшей конвертации берется полученный остаток [lala](#) и добавляется к концу path паттерна из поля **Изменить на**, то есть: [/ad/test](#) + [lala](#). В итоге, после преобразования, параметр path получает значение [/ad/testlala](#).

Таким образом, конечный запрос будет отправлен по адресу [test.dev/ad/testlala](#).

2) Запрос на [test.dev/exa/vvv](#).

Параметр path = [/exa/vvv](#). Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается [/exa](#). Оставшаяся часть: [/vvv](#).

При дальнейшей конвертации берется полученный остаток [/vvv](#) и добавляется к концу path паттерна из поля **Изменить на**, то есть: [/ad/test](#) + [/vvv](#). В итоге, после преобразования, параметр path получает значение [ad/test/vvv](#).

Таким образом, конечный запрос будет отправлен по адресу [test.dev/ad/test/vvv](#).

