

Table of Contents

Table of Contents	1
Глобальный портал	2
Описание	3
Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси	4
Веб-портал (SSL VPN)	7

Описание

Documentation: ☒

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1

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: UserGate NGFW
Version: 7.0.1

Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси.

В отличие от публикации с помощью правил DNAT, публикация с использованием reverse-прокси предоставляет следующие преимущества:

- Публикация по HTTPS серверов, работающих по HTTP и наоборот.
- Балансировка запросов на ферму веб-серверов.
- Возможность ограничения доступа к публикуемым серверам с определенных Useragent.
- Возможность подмены доменов и путей публикуемых серверов.

Чтобы опубликовать сервер, используя reverse-прокси, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать сервер reverse-прокси.	В разделе Глобальный портал → Серверы reverse-прокси нажать на кнопку Добавить и создать один или более публикуемых веб-серверов.
Шаг 2. Создать правило балансировки на серверы reverse-прокси (опционально).	В случае, если требуется балансировка на ферму публикуемых серверов, создать в разделе Политики сети → Балансировка нагрузки балансировщик reverse-прокси. В качестве серверов используются серверы reverse-прокси, созданные на предыдущем шаге.
Шаг 3. Создать правило reverse-прокси.	В разделе Глобальный портал → Правила reverse-прокси создать правило, которое будет задавать условия публикации серверов или фермы серверов. Важно! Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в настройках правила.
Шаг 4. Разрешить сервис Reverse-прокси на зоне, с которой необходимо разрешить доступ к внутренним ресурсам.	В разделе Сеть → Зоны разрешите сервис Reverse-прокси для зоны, с которой необходимо разрешить доступ к внутренним ресурсам (обычно зона Untrusted).

Для создания сервера reverse-прокси разделе **Глобальный портал → Серверы reverse-прокси** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
Название	Название публикуемого сервера.
Описание	Описание публикуемого сервера.
Адрес сервера	IP-адрес публикуемого сервера.
Порт	TCP-порт публикуемого сервера.
HTTPS до сервера	Определяет, требуется ли использовать протокол HTTPS до публикуемого сервера.
Проверять SSL-сертификат	Включает/отключает проверку валидности SSL-сертификата, установленного на публикуемом сервере.
Не изменять IP-адрес источника	Оставляет оригинальный IP-адрес источника в пакетах, пересылаемых на публикуемый сервер. Если отключено, то IP-адрес источника заменяется на IP-адрес UserGate.

Для создания правила балансировки на серверы reverse-прокси в разделе **Политики сети → Балансировка нагрузки** необходимо выбрать **Добавить → Балансировщик reverse-прокси** и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Серверы reverse-прокси	Созданный на предыдущем шаге список серверов reverse-прокси, на которые будет распределяться нагрузка.

Для создания правила reverse-прокси необходимо нажать на кнопку **Добавить** в разделе **Глобальный портал → Правила reverse-прокси** и заполнить необходимые поля.

Примечание Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Низе**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

Примечание Флажок *Инvertировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Сервер reverse-прокси	Сервер reverse-прокси или балансировщик reverse-прокси, куда NGFW будет пересылать запросы.
Порт	Порт, на котором NGFW будет слушать входящие запросы.
Использовать HTTPS	Включает поддержку HTTPS.
Сертификат	Сертификат, используемый для поддержки HTTPS-соединения.
Авторизовать 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. Более подробно о пользовательских сертификатах читайте в разделе Управление сертификатами .
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.

Наименование	Описание
Пользователи	Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Данная вкладка доступна только при использовании HTTPS и авторизации пользователя по сертификату.
Назначение	Адрес назначения должен быть назначен на интерфейс, на который приходит входящее соединение. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.
Useragent	UserAgent пользовательских браузеров, для которых будет применено данное правило.
Подмена путей	Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на http://www.example.com/path1 в http://www.example.loc/path2 Изменить с - домен и/или путь URL, которые требуется изменить. Изменить на - домен и/или путь URL, на которые требуется заменить старые. Если указан домен в поле Изменить с, то правило публикации будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.

Documentation: ☒
Product: NGFW
Version: 7.0.1

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).

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. Более подробно о профилях аутентификации смотрите раздел руководства Профили аутентификации .
Шаблон страницы аутентификации	Выбрать шаблон страницы аутентификации, который будет использоваться для отображения формы для ввода логина и пароля. Создать свою страницу аутентификации можно в разделе Шаблоны страниц .
Шаблон портала	Выбрать шаблон веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Создать свою страницу аутентификации можно в разделе Шаблоны страниц .
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.

Наименование	Описание
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробно о профилях SSL смотрите в главе 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. Более подробно о ролях сертификатов смотрите в разделе руководства 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. Более подробно о пользовательских сертификатах читайте в разделе Управление сертификатами .

Настройке 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 gdr:// . 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.
Иконка	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из предопределенных 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.

