

Table of Contents

Table of Contents	1
Правила фильтрации	2
Как ограничить полосу пропускания группе пользователей для доступа к видео из сети Интернет	3
Как запретить трафик для определенных приложений	5
Как разрешить работу клиента Dropbox	6
Не удастся настроить исключение блокировки рекламы	8
Не работают правила, содержащие ограничения по внешним пользователям	9
Разделение трафика для применения разных алгоритмов обработки	10
При включении DNS-фильтрации начинают блокироваться разрешенные ресурсы	11
Исключение трафика конкретных приложений из проксирования и инспектирования	12
Взаимодействие правил reverse-прокси, DNAT и межсетевого экрана	13
Запретить NAT "серых" IP адресов	14
Некорректная работа Яндекс Браузера с сервисами Google	16

KnowledgeBase: 

Product: UserGate NGFW

Задача

Необходимо ограничить группе пользователей локальной сети полосу пропускания для доступа к видеоконтенту из сети Интернет и не ограничивать полосу пропускания для доступа к серверам компании, расположенным в зоне DMZ.

Решение

Правила пропускной способности работают только с исходящим от UserGate трафиком, на входящий трафик UserGate влиять не может, поэтому принимает весь трафик.

Особенность настройки заключается в том, что правило пропускной способности будет работать только для зоны назначения и будет не работать для зоны источника, поэтому в правилах указываются **Адрес источника** и **Зона назначения**.

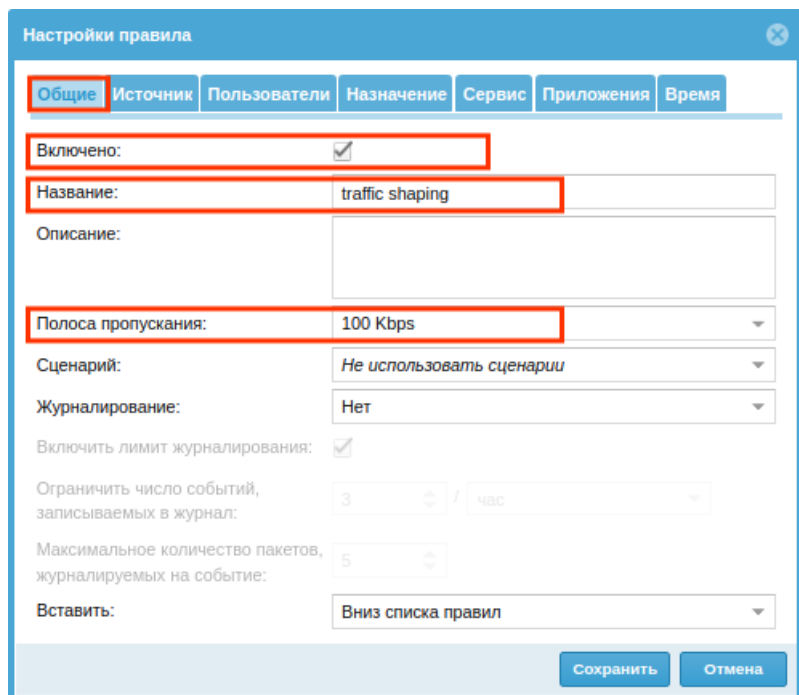
На UserGate настроена зона **Trusted**, назначенная для интерфейса, через который пользователи локальной сети получают доступ в Интернет. Также произведена настройка зоны **DMZ**, в которой расположены различные сервера компании, используемые для предоставления ресурсов пользователям локальной сети.

1. Создать правило для ограничения полосы пропускания.

В разделе **Политики сети** → **Пропускная способность** нажмите кнопку **Добавить** и создайте правило. В свойствах укажите необходимые данные.

Во вкладке **Общие**:

- **Название правила.**
- **Полоса пропускания:** 100 Kbps.



Настройки правила

Общие | Источник | Пользователи | Назначение | Сервис | Приложения | Время

Включено: ☒

Название: traffic shaping

Описание:

Полоса пропускания: 100 Kbps

Сценарий: Не использовать сценарии

Журналирование: Нет

Включить лимит журналирования: ☒

Ограничить число событий, записываемых в журнал: 3 / час

Максимальное количество пакетов, журналируемых на событие: 5

Вставить: Вниз списка правил

Сохранить Отмена

Во вкладке **Назначение** в разделе **Зона назначения** укажите **Trusted**.

Как запретить трафик для определенных приложений

Product: UserGate NGFW

Задача

Необходимо запретить или разрешить трафик для определенных приложений

Решение

Перейдите в раздел **Политики сети → Межсетевой экран**. Создайте правило и укажите приложения, к которым оно должно применяться (в свойствах правила перейдите во вкладку **Приложения** и нажмите **Добавить → Добавить приложения**).

Помимо отдельных приложений можно указать:

- **Все группы приложений**.
- **Группы приложений**: выберите группы приложений, к которым необходимо применить правило межсетевого экрана (добавление групп описано далее).
- **Категории приложений**: выберите категории приложений, к которым необходимо применить правило межсетевого экрана (например, Games, Web browsing и т.п.).

Чтобы создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика:

1. Перейдите в раздел **Библиотеки → Приложения**, на панели **Группы приложений** нажмите кнопку **Добавить**. Далее укажите название и описание группы приложений.
2. Добавьте приложения в созданную ранее группу, нажав на панели **Приложения** кнопку **Добавить** и выбрав нужные приложения.

Примечание Для идентификации приложения необходимо, чтобы соединение между клиентом и сервером было установлено и прошла какая-то часть трафика в обоих направлениях.

Объем такого трафика ограничен 1кб

Поэтому под правило, разрешающее приложение, может попасть любой трафик, удовлетворяющий остальным критериям в правиле, до того момента, когда приложение будет идентифицировано.

Аналогично, запрещающее правило по приложению сработает (разорвет сессию) только после завершения идентификации приложения.

Как разрешить работу клиента Dropbox

Product: UserGate NGFW

KnowledgeBase: ☒

Задача

Необходимо разрешить работу клиента Dropbox

Решение

Для организации работы клиента Dropbox необходимо создать новое правило дешифрования в разделе **Политики безопасности → Инспектирование SSL**. Укажите необходимые данные.

Во вкладке **Общие** укажите:

- **Название** правила инспектирования.
- **Действие** - **Не расшифровывать**.

Свойства правила инспектирования SSL

Общие Пользователи Источник Адрес назначения Сервисы Категории Домены Время

Включено: ☒

Название: for Dropbox

Описание:

Действие: Не расшифровывать

Профиль SSL: Default SSL profile

Записывать в журнал правил: ☒

Атрибуты:

- ☐ Блокировать сайты с некорректными сертификатами
- ☐ Проверять по списку отозванных сертификатов
- ☐ Блокировать сертификаты с истекшим сроком действия
- ☐ Блокировать самоподписанные сертификаты

Вставить: Наверх списка правил

Сохранить Отмена

В разделе **Библиотеки → Списки URL** создайте новый список и добавьте следующие сайты:

- www.dropbox.com
- client.dropbox.com
- client-web.dropbox.com
- d.dropbox.com
- block-edge-1.dropbox.com
- dl-debug.dropbox.com
- bolt.dropbox.com
- api.dropboxapi.com
- clientupdates.dropboxstatic.com
- cfl.dropboxstatic.com
- www.google.com
- www.gstatic.com

Список URL также можно создать при настройке правила во вкладке **Домены** (кнопка **Создать и добавить новый объект**).

Создать новый список URL

Название списка:

URL обновления:

Адреса URL

[+ Добавить](#) [✎ Редактировать](#) [✖ Удалить](#)

URL
www.dropbox.com
client.dropbox.com
client-web.dropbox.com
d.dropbox.com
block-edge-1.dropbox.com
dl-debug.dropbox.com
bolt.dropbox.com
api.dropboxapi.com
clientupdates.dropboxstatic.com
cfi.dropboxstatic.com
www.google.com
www.gstatic.com

[Сохранить](#) [Отмена](#)

Последние два URL требуются только для возможности первоначально авторизоваться в клиенте Dropbox с реквизитами учётной записи из Google. Если их не указывать, то первичная авторизация, независимо от типа учётной записи, будет произведена не в клиенте Dropbox, а в браузере по умолчанию. Для последующей работы клиента Dropbox эти URL не требуются.

Далее во вкладке **Домены** свойств правила инспектирования укажите созданный ранее список URL.

Свойства правила инспектирования SSL

Общие Пользователи Источник Адрес назначения Сервисы Категории **Домены** Время

[+ Добавить](#) [✎ Редактировать](#) [✖ Удалить](#)

URL	Владелец
 for dropbox	Вы

[Создать и добавить новый объект](#)

☐ Инvertировать

[Сохранить](#) [Отмена](#)

Примечание Данное правило необходимо расположить в начале списка правил инспектирования SSL.

Не удается настроить исключение блокировки рекламы

Technology: SSL Inspection

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Задача

При попытке зайти на необходимый сайт выдается страница блокировки. Попытка создать исключение для правил блокировки рекламы ни к чему не приводит, сайт по-прежнему блокируется.

Решение

Одной из возможных причин такого поведения является несоответствие алгоритмов шифрования, которые выбирает сервер алгоритмам, поддерживаемым браузером. Иными словами сервер может выбрать алгоритм шифрования, который не поддерживается браузером, но присутствует профиле инспектирования SSL. Большинство сайтов прекрасно работают при использовании **SSL-профиля по умолчанию**, тем не менее, чтобы исключить конфликт, можно посмотреть какие алгоритмы шифрования выбирает сервер и поддерживает браузер. Для этого нужно записать трафик между браузером и сервером и внести в настройки профиля инспектирования SSL только те алгоритмы, которые поддерживает браузер на вкладке: **Свойства SSL-профиля → Общие**

Не работают правила, содержащие ограничения по внешним пользователям

Product: UserGate NGFW

Задача

Не работают правила, содержащие ограничения по пользователям, полученным с внешних серверов (например, LDAP-коннектора).

Решение

Возможны несколько причин возникновения данной проблемы.

Возможная причина №1

Для того чтобы пользователей можно было использовать в правилах любого модуля, пользователи должны пройти аутентификацию одним из поддерживаемых методов (подробнее читайте в соответствующем [разделе](#) руководства администратора).

Примечание Для использования пользователей в правилах межсетевого экрана в соответствующем captive-профиле, если используется не агент аутентификации, в качестве метода идентификации необходимо указать Запоминать IP-адрес.

Возможная причина №2

Случай асимметричного трафика: пакет от клиента к серверу передаётся через UserGate, а обратный - напрямую к клиенту (без обработки на UserGate). В этом случае межсетевой экран с контролем состояния обратный пакет не привязывает к пользователю. В такой ситуации необходимо правильно настроить маршрутизацию трафика, чтобы все пакеты шли через UserGate либо настроить правило SNAT для отправки такого трафика от имени UserGate.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Задача

Необходимо разделить трафик пользователей: для одних пользователей UserGate должен работать в режиме явного прокси (Explicit Proxy Mode), для других - в режиме прозрачного прокси (Transparent Proxy Mode). Трафик от всех пользователей поступает на один интерфейс.

Решение

Поскольку весь трафик пользователей поступает на один интерфейс, UserGate автоматически применяет политики безопасности ко всему трафику с портами назначения 80 и 443.

Для разделения трафика выполните следующие действия:

1. Направьте трафик на разные интерфейсы (т.е. трафик, к которому должны быть применены политики UserGate направьте на один интерфейс, трафик, который должен пройти через UserGate без анализа - на другой); назначьте им разные зоны. Это позволит разделять трафик по признаку зоны источника.

Чтобы назначить двум интерфейсам адреса из одной сети (если нет другого маршрутизатора, на котором можно было бы выделить отдельную сеть), создайте для интерфейса, который будет указан как явный прокси, отдельный виртуальный маршрутизатор. В нём необходимо указать маршруты и шлюзы, аналогичные маршрутам и шлюзам маршрутизатора по умолчанию.

2. Для зоны источника интерфейса, указанного как шлюз по умолчанию, настройте разрешающие правила инспектирования SSL и фильтрации контента; расположите эти правила в начале списка.

Подробнее об алгоритме обработки трафика в UserGate версии 6.x.x читайте в статье [UserGate NGFW 6 Packet Flow](#).

При включении DNS-фильтрации начинают блокироваться разрешенные ресурсы

Product: UserGate NGFW
Technology: Content Filtering
Version: 5.x, 6.x, 7.x

Задача

При включении DNS-фильтрации начинают блокироваться разрешенные ресурсы.

Решение

Возможно в вашей сети используются интерфейсы типа L2 мост. К сожалению, в текущей версии UserGate NGFW функционалы DNS фильтрации и моста L2 несовместимы, в результате при включении DNS фильтрации, DNS запросы через L2 мост работать не могут.

Задача

Некоторые приложения некорректно работают при использовании устройств MITM. Требуется исключить их из проксирования и инспектирования.

Решение

Данная проблема решается путем исключения трафика проблемных приложений из проксирования и SSL инспектирования, для этого необходимо:

1. Создать список URL, содержащий доменные адреса, к которым подключаются проблемные сервисы.
2. Настроить правило captive-портала с действием "Не использовать аутентификацию" и указать созданный список URL. Правило необходимо поместить выше правила captive-портала, предназначенного для авторизации.
3. Настроить SSL-инспектирование с действием "Не расшифровывать" для созданного списка URL. Правило следует поместить выше правила расшифровки.
4. Настроить разрешающее правило контентной фильтрации для созданного списка URL и поместить его выше остальных правил.

Журналирование для всех перечисленных правил нужно выключить.

Technology: Content Filtering

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Интересует вопрос: как и на сколько корректно будут работать правила reverse-прокси, DNAT и Межсетевого Экрана, если везде в них будет фигурировать один и тот же IP адрес.

Ответ

Использование одного адреса для публикации разных сервисов - это общепринятая практика. Каждое правило публикации перенаправляет соединения в соответствии с указанными в его настройках протоколами и портами.

ПО UserGate позволяет использование правил reverse-прокси для публикации одних портов и правил DNAT для других на одном общем адресе. В правилах reverse-прокси TCP-порт (или список портов) указывается в соответствующем поле на вкладке Общие, а в правиле DNAT протоколы и порты определяются сервисами выбранными на соответствующей вкладке. Если будет указан один и тот же порт для правил DNAT и reverse-прокси, то правила DNAT сработает первым и правило reverse-прокси не сработает.

Правила межсетевого экрана в данном случае могут выполнять роль дополнительного фильтра, т.е. запрещать часть соединений автоматически разрешаемых правилами reverse-прокси и DNAT.

Более подробно о правилах прохождения пакетов через ПО UserGate можно посмотреть [здесь](#).

Запретить NAT "серых" IP адресов

Technology: Firewall
Version: 7.0.0, 7.0.1, 7.0.2, 7.1.0, 6.x
Product: UserGate NGFW

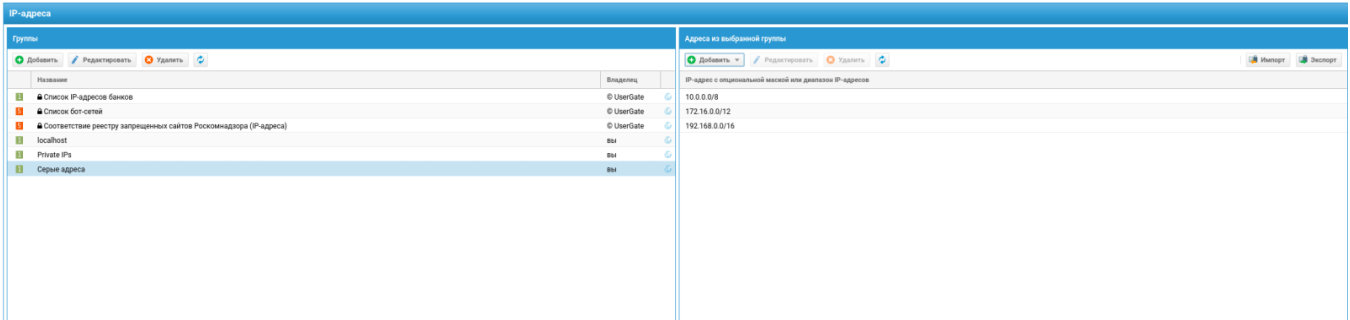
Задача

Необходимо запретить NAT трансляцию серых адресов.

Решение

Для решения задачи необходимо выполнить следующие шаги:

1. Добавить список запрещенных для NAT IP-адресов. Для этого по пути: **Библиотеки → IP-адреса**, нужно добавить список запрещенных для NAT адресов.



2. В правилах NAT добавить данный список в качестве **Источника** или **Назначения** с установкой флага **Инвертировать**. Для этого: по пути: **Политики сети → NAT** и маршрутизация, добавить правило NAT или отредактировать существующее. Открыть настройки **Источника** и/или **Назначения**, и добавить запрещенные адреса с флагом **Инвертировать**.

Свойства правила

Общие

Источник

Пользователи

Назначение

Сервис

Порт-форвардинг

DNAT

Network mapping

Использование

История

Зона источника

☐ Cluster

☐ DMZ

☐ Management

☒ Trusted

☐ Tunnel inspection zone

☐ Untrusted

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается «любая зона»

Создать и добавить новый объект

☐ Инвертировать

Адрес источника

+ Добавить

Редактировать

Удалить

Название списка ↑

Владелец

Серые адреса

Вы

Создать и добавить новый объект

☒ Инвертировать

Сохранить

Отмена

Некорректная работа Яндекс Браузера с сервисами Google

Technology: Content Filtering

Version: 6.x, 7.x

Product: UserGate NGFW

Задача

Некорректная работа через Яндекс Браузер с сервисами Google, при этом на устройстве UserGate есть разрешающее правило для работы Яндекс Браузера.

Решение

Проблема скорее всего связана с этим:

«Разработчики Яндекса случайно обнаружили, что в драйверах AMD есть оптимизация под Chrome, но нет исправлений для других браузеров, основанных на Chromium. Компания уже направила запрос в AMD, но пока, чтобы не ждать, программисты просто встроили в Яндекс Браузер функцию мимикрии под Chrome — количество падений GPU-процесса снизилось в 5,5 раз, расход памяти уменьшился на 8%.»

Яндекс Браузер при работе с сервисами Google меняет свой User-Agent на Chrome, из-за чего могут происходить ложные срабатывания правил и другие артефакты обработки трафика. Это можно нивелировать с помощью средств разработчика, путем установки в браузере кастомизированного User-Agent на любую (даже не существующую) версию Яндекс Браузера. При этом отключается механизм подмены своего User-Agent в Яндекс Браузере.

