

## Table of Contents

|                              |    |
|------------------------------|----|
| Table of Contents            | 1  |
| Библиотеки элементов         | 2  |
| Общие сведения               | 3  |
| Морфология                   | 4  |
| Сервисы                      | 7  |
| Группы сервисов              | 9  |
| IP-адреса                    | 10 |
| Useragent браузеров          | 12 |
| Типы контента                | 13 |
| Списки URL                   | 15 |
| Календари                    | 18 |
| Полосы пропускания           | 19 |
| Шаблоны страниц              | 20 |
| Категории URL                | 22 |
| Измененные категории URL     | 28 |
| Приложения                   | 29 |
| Профили приложений           | 32 |
| Группы приложений            | 39 |
| Почтовые адреса              | 40 |
| Номера телефонов             | 41 |
| Сигнатуры COB                | 42 |
| Профили COB                  | 50 |
| Профили оповещений           | 55 |
| Профили Netflow              | 56 |
| Профили LLDP                 | 57 |
| Профили SSL                  | 58 |
| Профили пересылки SSL        | 60 |
| NIP объекты                  | 61 |
| NIP-профили                  | 63 |
| Профили BFD                  | 64 |
| Syslog-фильтры UserID агента | 66 |
| Сценарии                     | 67 |
| Теги                         | 73 |



## Общие сведения

---

Version: 7.x

Product: NGFW

Documentation: 

Библиотеки элементов содержит в себе все записи, адреса сайтов, IP-адреса, шаблоны, сигнатуры и прочие элементы, которые используются при настройке правил UserGate NGFW.

Первоначальные данные библиотек поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Некоторые элементы библиотек являются нередактируемыми, потому что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, обновляются автоматически при наличии специальной лицензии. Подробнее о лицензировании — в разделе «[Лицензирование UserGate NGFW](#)».

Морфология

Product: NGFW  
Version: 7.x  
Documentation: 

Морфологический анализ — механизм, который распознает отдельные слова и словосочетания на веб-сайте. Если в тексте содержится достаточное для блокировки количество указанных слов и словосочетаний, то доступ к сайту блокируется.

Морфологический анализ выполняется как при проверке запроса пользователя, так и при получении ответа от веб-сервера и до его передачи пользователю. Получив ответ от веб-сервера, NGFW просматривает текст на странице и подсчитывает его суммарный «вес», исходя из «весов» слов, указанных в морфологических категориях. Если «вес» страницы превышает «вес» морфологической категории, правило срабатывает. При подсчете «веса» страницы учитываются все словоформы (леммы) запрещенных слов. Для поиска словоформ NGFW использует встроенные словари русского, английского, японского, арабского и немецкого языков.

Существует возможность подписки на словари, предоставляемые UserGate. Данные словари нельзя редактировать. Для использования этих словарей необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование](#).

| Наименование                                                                          | Описание                                                                                                          |
|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Соответствие списку запрещенных материалов Министерством Юстиции Российской Федерации | Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции Российской Федерации. |
| Соответствие списку запрещенных материалов республики Казахстан                       | Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции республики Казахстан. |
| Суицид                                                                                | Морфологический словарь, содержащий перечень слов и фраз суицидальной направленности.                             |
| Терроризм                                                                             | Морфологический словарь, содержащий перечень слов и фраз террористической направленности.                         |
| Нецензурная лексика                                                                   | Морфологический словарь, содержащий перечень слов и фраз, относящихся к нецензурной лексике.                      |
| Азартные игры                                                                         | Морфологический словарь, содержащий перечень слов и фраз, относящихся к азартным играм.                           |
| Наркотики                                                                             | Морфологический словарь, содержащий перечень слов и фраз наркотической направленности.                            |
| Соответствие ФЗ-436 (Защита детей)                                                    | Морфологический словарь, содержащий перечень слов и фраз тематик, нежелательных для детей.                        |
| Порнография                                                                           | Морфологический словарь, содержащий перечень слов и фраз порнографической направленности.                         |
| Бухгалтерия (DLP)                                                                     | Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в бухгалтерии.                   |
| Маркетинг (DLP)                                                                       | Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в маркетинге.                    |
| Персональные данные (DLP)                                                             | Морфологический словарь, содержащий перечень терминов, слов и фраз, встречающихся в персональных данных.          |
| Финансы (DLP)                                                                         | Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в финансах.                      |
| Юридический (DLP)                                                                     | Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в юриспруденции.                 |

Для фильтрации по морфологическому содержанию страницы требуется:

| Наименование                                                                                | Описание                                                                     |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Шаг 1. Создать одну или несколько морфологических категорий и указать вес каждой категории. | Нажать на кнопку <b>Добавить</b> , задать название новой категории и ее вес. |

| Наименование                                                                                                | Описание                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 2.</b> Указать список запрещенных фраз с весами.                                                     | Нажать на кнопку <b>Добавить</b> и указать необходимые слова или фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки. |
| <b>Шаг 3.</b> Создать правило фильтрации контента, содержащее одну или несколько морфологических категорий. | Смотрите раздел <a href="#">Фильтрация контента</a> .                                                                                                                                                                                                                                                                               |

Администратор имеет возможность создать свой словарь и централизованно распространять его на все межсетевые экраны UserGate, имеющиеся в организации. Для создания такой морфологической базы необходимо выполнить следующие действия:

| Наименование                                                                        | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать файл с необходимыми фразами.                                  | создать файл <b>list.txt</b> со списком слов в следующем формате:<br><br>!word1 !word2<br><br>!word3<br><br>word4 50<br><br>...<br><br>Lastword<br><br>Вес словаря в таком случае равен 100, вес слова можно указать. По умолчанию он равен 100.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Шаг 2.</b> Создать архив, содержащий этот файл.                                  | Поместить файл в архив zip с именем <b>list.zip</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Шаг 3.</b> Создать файл с версией словаря.                                       | Создать файл <b>version.txt</b> , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Шаг 4.</b> Разместить файлы на веб-сервере.                                      | Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Шаг 5.</b> Создать морфологическую категорию указать URL для обновления словаря. | <p>На каждом UserGate создать морфологическую базу. При создании указать тип списка <b>Обновляемый</b> и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:</p> <ul style="list-style-type: none"> <li>Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.</li> <li>Ежедневно.</li> <li>Еженедельно.</li> <li>Ежемесячно.</li> <li>Каждые ... часов.</li> <li>Каждые ... минут.</li> <li>Задать вручную.</li> </ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"> <li>Звездочка (*) — обозначает весь диапазон (от первого до последнего).</li> <li>Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.</li> <li>Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li> <li>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".</li> </ul> |

**Примечание** При создании морфологических словарей не рекомендуется добавлять фразы, содержащие более трех слов, без использования символа «!» перед словами. Необходимо помнить, что при построении морфологической базы каждое из слов будет преобразовано во все существующие формы (склонения, спряжения, множественные числа, времена и т.д.), и результирующее количество фраз будет достаточно большим. При добавлении длинных фраз необходимо использовать модификатор «!» перед словами, модификация которых не нужна, как правило, это различные предлоги и союзы. Например, фразу «как уйти из жизни безболезненно» правильно добавить в виде «!как уйти !из !жизни безболезненно». Это сократит количество возможных вариантов фраз, но при этом оставит все фразы с требуемым смыслом.

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Version: 7.x

Product: NGFW

Documentation: 

Раздел **Сервисы** содержит список общеизвестных сервисов, основанных на протоколах TCP/IP, например, таких как HTTP, HTTPS, FTP и другие. Эти сервисы могут быть использованы при построении правил NGFW. Первоначальный список сервисов поставляется вместе с продуктом.

Вы можете добавлять необходимые вам элементы в процессе работы. Чтобы добавить новый сервис:

1. В веб-консоли UserGate NGFW перейдите в раздел **Настройки → Библиотеки → Сервисы** и нажмите **Добавить**.
2. В открывшемся окне свойств сервиса укажите название и произвольное описание сервиса
3. Нажмите **Добавить**, выберите необходимый сетевой протокол и укажите порты сервиса. Порты можно указывать диапазонами, например, 33333-33355:

При выборе сетевых протоколов TCP или UDP можно также выбрать шлюз прикладного уровня (Application Layer Gateway — ALG).

Некоторые протоколы используют отдельные потоки для обмена сигнальной информацией и передачи данных. Примерами таких протоколов являются FTP, SIP или H.323. Параметры установления потока передачи данных (например, IP-адреса или порты) у таких протоколов не настраиваются заранее, а согласуются при обмене сигнальными сообщениями между устройствами на этапе активации сервиса. Для управления такими протоколами в UserGate NGFW используются шлюзы прикладного уровня (ALG).

ALG работает как посредник между сетью и сервером приложений, который понимает прикладной протокол. Например, ALG может разрешать клиентским приложениям использовать динамические порты TCP/UDP для взаимодействия с известными портами, используемыми серверными приложениями, даже в тех случаях, когда настройки межсетевого экрана разрешают трафик только через ограниченное число портов. Без ALG порты будут блокироваться, либо администраторам придется открывать в межсетевом экране большое количество портов, что ослабляет безопасность сети и открывает возможность для потенциальных атак через эти порты. Также ALG может распознавать конкретные команды приложения и получать адресную информацию сетевого уровня, которая находится в пэйлоаде пакетов приложения. ALG может синхронизировать несколько потоков или сеансов между хостами.

При создании нового сервиса с протоколом TCP можно выбрать шлюзы прикладного уровня для следующих протоколов:

- FTP;
- SIP;
- H.323.

При создании нового сервиса с протоколом UDP можно выбрать шлюзы прикладного уровня для протоколов:

- SIP;
- FTFTP.

FTP использует несколько потоков для передачи файлов — первичный сигнальный поток и вторичные потоки данных для списков каталогов и передачи файлов. Поскольку эти потоки данных могут подключаться к любому порту, сложно создать статическую политику межсетевого экрана, которая бы разрешала эти потоки данных и при этом обеспечивала адекватную защиту. FTP ALG автоматически решает эту проблему путем мониторинга сигнального потока FTP, поиска команд порта FTP, которые указывают, какие порты источника и назначения запрашиваются. ALG динамически открывает определенную комбинацию IP-портов источника и назначения в политике межсетевого экрана, которая позволяет установить сессию. Как только сессия завершена, шлюз немедленно закрывается. В случае, если FTP-сессия проходит через NAT, ALG анализирует пакеты на прикладном уровне, заменяя внутренний IP на адрес интерфейса NAT.

SIP ALG — шлюз прикладного уровня, который позволяет голосовому VoIP-трафику (RTP) проходить через устройство с функцией NAT. Если на межсетевом экране присутствует и активирован SIP ALG, то не нужно дополнительно настраивать проброс портов для этого типа трафика. Для беспрепятственного прохождения SIP-трафика через устройство с NAT необходимо транслировать адресацию в SIP-пакетах. SIP-пакет анализируется на прикладном уровне, и в нем изменяются IP-адреса. Так SIP ALG позволяет реализовать услуги SIP-телефонии в сети с трансляцией адресов без использования вспомогательных внешних устройств.

H.323 ALG поддерживает набор протоколов H.225.0 и H.245 для обеспечения сеанса аудиовизуальной связи в сети. ALG позволяет трафику проходить через устройство с функцией NAT, анализируя пакеты на уровне приложения, и заменяя в них IP-адреса.

По умолчанию шлюзы прикладного уровня отключены в параметрах устройства. Включить их можно в интерфейсе командной строки (CLI) с помощью следующей команды:

```
Admin@nodename# set settings device <sip|h323|ftp-alg> on
```

Подробнее — в разделе [Настройка параметров устройства](#).

## Группы сервисов

---

Version: 7.x

Product: NGFW

Documentation: 

В этом разделе вы можете управлять (создавать, обновлять, удалять) группами объектов сервисов. Группы сервисов могут быть использованы при настройке политик безопасности NGFW.

Для создания группы сервисов:

1. В разделе **Настройки → Библиотеки → Группы сервисов** в блоке **Группы сервисов** нажмите **Добавить** и укажите название и произвольное описание создаваемой группы.
2. В блоке **Элементы** нажмите **Добавить** и выберите сервисы для добавления в группу. Для добавления всех сервисов нажмите **Добавить все**.

Version: 7.x  
Product: NGFW  
Documentation: 

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил NGFW. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

| Наименование                                                             | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать список.                                            | На панели <b>Группы</b> нажать на кнопку <b>Добавить</b> : <ul style="list-style-type: none"><li>• Дать название списку IP-адресов.</li><li>• Добавить описание списка (опционально).</li><li>• Указать уровень угрозы адресов в списке (параметр для визуального отображения, какие адреса не представляют собой угрозы, а какие лучше запретить).</li><li>• Выбрать тип списка (локальный или обновляемый по URL обновления).</li></ul> |
| <b>Шаг 2.</b> Указать адрес обновления списка (для обновляемых списков). | Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе.                                                                                                                                                                                                                                                                                                               |
| <b>Шаг 3.</b> Добавить IP-адреса.                                        | На панели <b>Адреса из выбранной группы</b> нажать на кнопку <b>Добавить</b> и ввести адреса.<br><br>IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.                                                                                                                                                                                |

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

| Наименование                                           | Описание                                                                                                                                                                                                           |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать файл с необходимыми IP-адресами. | Создать файл <b>list.txt</b> со списком адресов.<br><br>Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например:<br>x.x.x.x<br>y.y.y.y<br>z.z.z.z |
| <b>Шаг 2.</b> Создать архив, содержащий этот файл.     | Поместить файл в архив zip с именем <b>list.zip</b> .                                                                                                                                                              |
| <b>Шаг 3.</b> Создать файл с версией списка.           | Создать файл <b>version.txt</b> , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.                                                  |
| <b>Шаг 4.</b> Разместить файлы на веб-сервере.         | Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.                                                                                                          |

| Наименование                                                   | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Шаг 5. Создать список IP-адресов и указать URL для обновления. | <p>На каждом NGFW создать список IP-адресов. При создании указать тип списка <b>Обновляемый</b> и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений.</p> <p><b>Примечание</b> URL списка задается в формате: http://x.x.x.x/, https://x.x.x.x/ или ftp://x.x.x.x/. При использовании протокола HTTPS требуется использовать сертификат, подписанный доверенным УЦ.</p> <p>Расписание можно настроить в свойствах списка; возможно указать следующие варианты:</p> <ul style="list-style-type: none"> <li>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.</li> <li>• Ежедневно.</li> <li>• Еженедельно.</li> <li>• Ежемесячно.</li> <li>• Каждые ... часов.</li> <li>• Каждые ... минут.</li> <li>• Задать вручную.</li> </ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"> <li>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).</li> <li>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7.</li> <li>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li> <li>• Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа".</li> </ul> |

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Useragent браузеров

Version: 7.x  
Product: NGFW  
Documentation:

С помощью фильтрации по Useragent браузеров администратор может запретить или разрешить работу пользователей только с определенным типом браузеров.

Первоначальный список Useragent поставляется вместе с продуктом. Для фильтрации по типу Useragent необходимо выполнить следующие действия:

| Наименование                                                                              | Описание                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать список Useragent.                                                   | В панели <b>Категории</b> нажать на кнопку <b>Добавить</b> и задать название нового списка UserAgent, опционально, описание списка и URL обновления.                                                                                                    |
| <b>Шаг 2.</b> Добавить необходимые Useragent браузеров в новый список.                    | В панели <b>Шаблоны useragent</b> добавить необходимый Useragent. Искерпывающий список строк Useragent представлен тут: <a href="http://www.useragentstring.com/pages/useragentstring.php">http://www.useragentstring.com/pages/useragentstring.php</a> |
| <b>Шаг 3.</b> Создать правило фильтрации контента, содержащее один или несколько списков. | Смотрите раздел <a href="#">Фильтрация контента</a> .                                                                                                                                                                                                   |

Администратор имеет возможность создавать свои списки Useragent и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

| Наименование                                                         | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать файл с необходимыми Useragent.                 | Создать файл <b>list.txt</b> со списком <b>Useragent</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Шаг 2.</b> Создать архив, содержащий этот файл.                   | Поместить файл в архив zip с именем <b>list.zip</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Шаг 3.</b> Создать файл с версией списка.                         | Создать файл <b>version.txt</b> , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Шаг 4.</b> Разместить файлы на веб-сервере.                       | Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Шаг 5.</b> Создать список Useragent и указать URL для обновления. | <p>На каждом NGFW создать список Useragent. При создании указать тип списка <b>Обновляемый</b> и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:</p> <ul style="list-style-type: none"><li>Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.</li><li>Ежедневно.</li><li>Еженедельно.</li><li>Ежемесячно.</li><li>Каждые ... часов.</li><li>Каждые ... минут.</li><li>Задать вручную.</li></ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"><li>Звездочка (*) — обозначает весь диапазон (от первого до последнего).</li><li>Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.</li><li>Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li><li>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".</li></ul> |

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

md5sum list.zip

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Типы контента

Version: 7.x  
Product: NGFW  
Documentation:

С помощью фильтрации типов контента можно блокировать загрузку файлов определенного типа, например, запретить все файлы типа \*.doc.

Существует возможность подписки на типы контента, предоставляемые разработчиками UserGate. Данные списки типов контента нельзя редактировать, их можно использовать при определении правил фильтрации контента. Для использования этих списков необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование](#).

Для фильтрации по типу контента необходимо выполнить следующие действия:

| Наименование                                                                                                         | Описание                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать список типов контента. Если используется предопределенный список UserGate, перейдите к шагу 3. | В панели <b>Категории</b> нажать на кнопку <b>Добавить</b> , задать название нового списка типа контента, опционально, описание списка и URL обновления.                                                                                                                                                                                                                          |
| <b>Шаг 2.</b> Добавить необходимые типы контента в новый список.                                                     | Добавить необходимый тип контента в данный список в формате MIME. Различные типы контента и их описание доступны по ссылке <a href="https://www.iana.org/assignments/media-types/media-types.xhtml">https://www.iana.org/assignments/media-types/media-types.xhtml</a> .<br>Например, для блокировки документов типа *.doc необходимо добавить тип контента «application/msword». |
| <b>Шаг 3.</b> Создать правило фильтрации контента, содержащее один или несколько списков.                            | Смотрите раздел <a href="#">Фильтрация контента</a> .                                                                                                                                                                                                                                                                                                                             |

Администратор имеет возможность создавать свои списки типов контента и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

| Наименование                                                             | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать файл с необходимыми типами контента.               | Создать файл <b>list.txt</b> со списком типов контента.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Шаг 2.</b> Создать архив, содержащий этот файл.                       | Поместить файл в архив zip с именем <b>list.zip</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Шаг 3.</b> Создать файл с версией списка.                             | Создать файл <b>version.txt</b> , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Шаг 4.</b> Разместить файлы на веб-сервере.                           | Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Шаг 5.</b> Создать список типа контента и указать URL для обновления. | <p>На каждом NGFW создать список типа контента. При создании указать тип списка <b>Обновляемый</b> и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:</p> <ul style="list-style-type: none"><li>Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.</li><li>Ежедневно.</li><li>Еженедельно.</li><li>Ежемесячно.</li><li>Каждые ... часов.</li><li>Каждые ... минут.</li><li>Задать вручную.</li></ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"><li>Звездочка (*) — обозначает весь диапазон (от первого до последнего).</li><li>Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.</li><li>Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li><li>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".</li></ul> |

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в Linux можно командой:

md5sum list.zip

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Списки URL

Product: NGFW  
Documentation: ☒  
Version: 7.x

Списки URL используются в правилах контентной фильтрации в качестве черных и белых списков.

Компания UserGate предоставляет ряд собственных обновляемых списков. Для использования этих списков необходима соответствующая лицензия. Подробнее о лицензировании UserGate NGFW — в разделе «[Лицензирование](#)».

| Наименование списка                                            | Описание                                                                                                                                                                                                                       |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Список поисковых систем без безопасного поиска                 | Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля                          |
| Соответствие списку запрещенных URL Министерства Юстиции РФ    | Список содержит URL, запрещенные Министерством Юстиции Российской Федерации                                                                                                                                                    |
| Соответствие списку запрещенных URL Республики Казахстан       | Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан                                                      |
| Список образовательных учреждений                              | Список доменных имен образовательных учреждений РФ                                                                                                                                                                             |
| Список фишинговых сайтов                                       | Список содержит URL фишинговых сайтов                                                                                                                                                                                          |
| Соответствие реестру запрещенных сайтов Роскомнадзора (URL)    | Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Список доступен на сайте <a href="http://eais.rkn.gov.ru">http://eais.rkn.gov.ru</a> |
| Соответствие реестру запрещенных сайтов Роскомнадзора (домены) | Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Список доступен на сайте <a href="http://eais.rkn.gov.ru">http://eais.rkn.gov.ru</a>                             |

Вы также можете создать собственные списки URL в веб-консоли или в [интерфейсе командной строки](#) UserGate NGFW.

Для создания списка в веб-консоли:

- В разделе **Настройки → Библиотеки → Списки URL** нажмите **Добавить** и задайте название и описание нового списка.
  - Выберите тип списка (локальный или обновляемый). Для обновляемого списка укажите URL обновления и настройте [расписание скачивания обновлений](#).
  - Установите категорию создаваемого списка в поле **Чувствительность к регистру**:
    - Чувствительный к регистру** — список URL-адресов, чувствительных к регистру букв в адресе.
    - Нечувствительный к регистру** — список URL-адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах.
    - Домен** — список адресов доменов. При добавлении в этот список записи вида `http://test.ru`, она будет преобразована в запись вида `test.ru`.
- Важно!** Категория списка задается при его создании. Изменить категорию после создания списка нельзя.
- Примечание!** При использовании URL-списка ищется весь URL запроса; при использовании доменного списка — только имя узла. При сохранении URL в доменный список в процессе преобразования из него удаляется все лишнее, остается только имя узла.
- Добавьте необходимые записи в новый список.

В списках можно использовать некоторые специальные символы. Значения специальных символов в списках:

- \* — любое количество любых символов;
- ^ — начало строки;
- \$ — конец строки.

Символы «?» и «#» не могут быть использованы в списках.

Правило фильтрации контента может содержать один или несколько списков. Подробнее — в разделе «[Фильтрация контента](#)».

**Внимание!** Спецсимволы не работают в списках исключений для блокировки рекламы. Не рекомендуется использовать спецсимволы в записях таких списков.

Если необходимо заблокировать строго определенный адрес, используйте символы начала ( ^ ) и конца ( \$ ) строки. Например:

`^http://domain.com/exacturl$`

Если необходимо заблокировать адрес и все страницы внутри него, используйте символ ^ в начале строки, без символа \$ в конце. Например:

`^http://domain.com/exacturl/`

Чтобы заблокировать домен со всеми возможными URL, укажите только имя домена без специальных символов:

`domain.com`

Примеры интерпретации URL-записей приведены в таблице.

| Пример записи                                  | Обработка DNS-запросов                                                                                                                                             | Обработка HTTP-запросов для списка доменов                                                                                                                                                                                                                                                                                                                                                        | Обработка HTTP-запросов для списков URL, чувствительных к регистру                                                                                                                                                                                                        | Обработка HTTP-запросов для списков URL, нечувствительных к регистру                                                                                                                                                                                  |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| yahoo.com<br>или<br>*yahoo.com*                | Блокируется весь домен и домены более высоких (3,4 и т.д.) уровней, например:<br><br>sport.yahoo.com;<br><br>mail.yahoo.com;<br><br>а также:<br><br>qweryyahoo.com | Блокируется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например:<br><br>http://sport.yahoo.com;<br><br>http://mail.yahoo.com;<br><br>https://mail.yahoo.com;<br><br>http://sport.yahoo.com/123;<br><br>http://qwertyyahoo.com/<br><br>http://qwertyyahoo.com/                                                                                          | Блокируются любые вхождения yahoo.com:<br><br>http://sport.yahoo.com;<br><br>http://mail.yahoo.com;<br><br>https://mail.yahoo.com;<br><br>http://sport.yahoo.com/123;<br><br>http://qwertyyahoo.com/<br><br>Не блокируются вхождения типа:<br><br>https://ya.ru/YAHoo.cOM | Блокируются любые вхождения yahoo.com:<br><br>http://sport.yahoo.com;<br><br>http://mail.yahoo.com;<br><br>https://mail.yahoo.com;<br><br>http://sport.yahoo.com/123;<br><br>http://qwertyyahoo.com/<br><br>https://ya.ru/YAHoo.cOM                   |
| ^mail.yahoo.com\$                              | Заблокирован только mail.yahoo.com                                                                                                                                 | Заблокированы:<br><br>http://mail.yahoo.com;<br><br>https://mail.yahoo.com;<br><br>а также любые ссылки на этом домене, например:<br><br>http://mail.yahoo.com/personal-finance<br><br>Т. е., блокируется весь домен mail.yahoo.com и все URL этого домена                                                                                                                                        | Ничего не заблокируется, поскольку URL должен начинаться с указания протокола                                                                                                                                                                                             | Ничего не заблокируется, поскольку URL должен начинаться с указания протокола                                                                                                                                                                         |
| ^mail.yahoo.com/\$                             | Ничего не заблокировано                                                                                                                                            | Заблокированы:<br><br>http://mail.yahoo.com;<br><br>https://mail.yahoo.com;<br><br>и любые ссылки на этом домене, например:<br><br>https://mail.yahoo.com/personal-finance<br><br>т. к. при преобразовании списка остается только домен, слеш в этом случае удалится и реально в списке будет:<br><br>^mail.yahoo.com\$<br><br>т. е. блокируется весь домен mail.yahoo.com и все URL этого домена | Ничего не заблокируется, поскольку URL должен начинаться с указания протокола                                                                                                                                                                                             | Ничего не заблокируется, поскольку URL должен начинаться с указания протокола                                                                                                                                                                         |
| ^https://finance.yahoo.com/personal-finance/\$ | Ничего не заблокировано                                                                                                                                            | Заблокированы:<br><br>http://finance.yahoo.com;<br><br>https://finance.yahoo.com;<br><br>и любые ссылки на этом домене, например:<br><br>http://finance.yahoo.com/personal-finance/<br><br>т.к. после преобразования в списке останется только:<br><br>^finance.yahoo.com\$<br><br>Т. е. блокируется весь домен finance.yahoo.com и все URL этого домена                                          | Заблокируется только запрос https://finance.yahoo.com/personal-finance/<br><br>Не заблокируется:<br><br>http://finance.yahoo.com/personal-finance/<br><br>и любое изменение регистра букв в URL:<br><br>https://finance.yahoo.com/personal-financeE/                      | Заблокируется только запрос https://finance.yahoo.com/personal-finance/<br><br>и любое изменение регистра букв в URL:<br><br>https://finance.yahoo.com/Personal-financeE/.<br><br>Не заблокируется:<br><br>http://finance.yahoo.com/personal-finance/ |

| Пример записи     | Обработка DNS-запросов  | Обработка HTTP-запросов для списка доменов                                                                                                                                                                         | Обработка HTTP-запросов для списков URL, чувствительных к регистру            | Обработка HTTP-запросов для списков URL, нечувствительных к регистру          |
|-------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| ^yahoo.com/12345/ | Ничего не заблокировано | Заблокированы:<br>http://yahoo.com/12345/whatever/;<br>https://yahoo.com/12345/whatever/;<br>т.к. после преобразования в списке будет:<br>^yahoo.com<br>Т. е. заблокируется домен yahoo.com и все URL этого домена | Ничего не заблокируется, поскольку URL должен начинаться с указания протокола | Ничего не заблокируется, поскольку URL должен начинаться с указания протокола |

Администратор имеет возможность создавать собственные обновляемые списки и централизованно распространять их на все узлы UserGate NGFW. Для создания таких списков выполните следующие действия:

1. Создайте текстовый файл (например, list.txt) со списком URL в следующем формате:

```
www.site1.com/url1
www.site2.com/url2
...
www.siteend.com/urlN
```

2. Создайте архив, содержащий этот файл (например, list.zip).
3. Создайте файл с версией списка (например, version.txt). Внутри файла укажите номер версии списка (например, 3). Необходимо инкрементировать это значение при каждом обновлении списка.
4. Разместите файлы архива и версии (например, list.zip и version.txt) на веб-сервере, чтобы они были доступны для скачивания.
5. На каждом UserGate NGFW создайте список URL. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate NGFW будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

**Примечание** URL списка задается в формате: http://x.x.x.x/, https://x.x.x.x/ или ftp://x.x.x.x/. При использовании протокола HTTPS требуется использовать сертификат, подписанный доверенным УЦ.

В свойствах списка можно настроить расписание обновления.

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (\*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

UserGate NGFW может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл list.zip.md5, содержащий чек-сумму файла list.zip. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в Linux можно с помощью команды:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш list.zip, после чего сохраняется с расширением .md5. Например, содержимое файла list.zip.md5:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Календари

Version: 7.x  
Product: NGFW  
Documentation: 

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах NGFW. Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

| Наименование                                     | Описание                                                                                                                |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Шаг 1. Создать календарь.                        | В панели <b>Группы</b> нажать на кнопку <b>Добавить</b> , указать название календаря и его описание.                    |
| Шаг 2. Добавить временные интервалы в календарь. | В панели <b>Элементы</b> нажать на кнопку <b>Добавить</b> и добавить интервал. Дать название интервалу и указать время. |

Version: 7.x  
Product: NGFW  
Documentation: 

Элемент библиотеки **Полоса пропускания** определяет скорость передачи данных, которую возможно в дальнейшем использовать в правилах управления полосой пропускания. Более подробно о правилах управления полосой пропускания смотрите в главе [Пропускная способность](#).

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления новой полосы пропускания необходимо выполнить следующие шаги:

| Наименование                                 | Описание                                                                                                 |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать полосу пропускания.    | Нажать на кнопку <b>Добавить</b> , дать название, описание.                                              |
| <b>Шаг 2.</b> Указать скорость.              | Указать скорость в Кбит/сек.                                                                             |
| <b>Шаг 3.</b> Указать значение DSCP для QoS. | Необязательный параметр. Если установлен, то будет прописываться в каждый IP пакет. Диапазон от 0 до 63. |

## Шаблоны страниц

Product: NGFW

Version: 7.x

Documentation: 

С помощью шаблонов страниц вы можете настраивать отображение страниц блокировки, авторизации, предупреждений и сетевых ошибок. Список шаблонов страниц, которые поставляются с UserGate NGFW, — см. в таблице ниже.

| Шаблон                                                                                 | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Blockpage (EN) и Blockpage (RU)</b>                                                 | Стандартные шаблоны блокировки на английском и русском языках. Подробнее о настройке этих шаблонов — в разделе ниже                                                                                                                                                                                                                                                                                                                                                  |
| <b>Captive portal user auth (EN) и Captive portal user auth (RU)</b>                   | Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль). При успешной авторизации пользователь получает доступ в интернет                                                                                                                                                                                                                                        |
| <b>Captive portal user auth + policy (EN) и Captive portal user auth + policy (RU)</b> | Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль), правила пользования сетью (соглашение об использовании), а также требует принять правила политики доступа. При успешной авторизации пользователь получает доступ в интернет                                                                                                                             |
| <b>Captive portal: email auth (EN) и Captive portal: email auth (RU)</b>               | Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе, подтвердив указанную электронную почту. Для корректной работы шаблонов необходимо настроить параметры раздела <b>Оповещения</b> в Captive-профиле                                                                                                                                               |
| <b>Captive portal: SMS auth (EN) и Captive portal: SMS auth (RU)</b>                   | Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя с помощью SMS. Для корректной работы шаблонов необходимо настроить параметры раздела <b>Оповещения</b> в Captive-профиле                                                                                                                                           |
| <b>Captive portal policy (EN) и Captive portal policy (RU)</b>                         | Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принять правила политики доступа. При согласии с политикой доступа пользователь получает доступ в интернет. Для работы шаблона требуется установить метод <b>Принять политику</b> в качестве метода аутентификации в Captive-профиле |
| <b>Captive portal user session (EN) и Captive portal user session (RU)</b>             | Шаблоны на английском и русском языках, с помощью которых пользователь может завершить свою авторизованную сессию, перейдя на страницу <a href="http://logout.captive">http://logout.captive</a> или <a href="http://USERGATE_IP/cps">http://USERGATE_IP/cps</a>                                                                                                                                                                                                     |
| <b>Content warning (EN) и Content warning (RU)</b>                                     | Шаблоны на английском и русском языках, содержащие страницу предупреждения, отображаемую при срабатывании правила контентной фильтрации с действием <b>Предупредить</b>                                                                                                                                                                                                                                                                                              |
| <b>FTP client (EN) и FTP client (RU)</b>                                               | Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP                                                                                                                                                                                                                                                                                                                                                                             |
| <b>SSL VPN (EN) и (RU)</b>                                                             | Шаблоны на английском и русском языках для отображения страницы веб-портала                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>SSL VPN RDP (EN) и (RU)</b>                                                         | Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал                                                                                                                                                                                                                                                                                                                                       |
| <b>SSL VPN SSH (EN) и (RU)</b>                                                         | Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал                                                                                                                                                                                                                                                                                                                                       |
| <b>TOTP INIT PAGE (EN) и TOTP INIT PAGE (RU)</b>                                       | Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей                                                                                                                                                                                                                                                                                                                                                  |
| <b>NETWORK ERROR PAGE (RU) и NETWORK ERROR PAGE (EN)</b>                               | Шаблоны на русском и английском языках для отображения страницы сетевых ошибок от прокси-сервера.<br>Доступны в версии ПО 7.4.0 и выше                                                                                                                                                                                                                                                                                                                               |

### Настройка шаблона страницы блокировки

По умолчанию шаблон страницы блокировки настроен на отображение следующей информации:

- Сведения о блокирующем правиле;
- Сведения об угрозе;

- Категория URL;
- Морфологические категории;
- Кнопка запроса добавления URL в белый список.

Но в HTML-коде шаблона страницы блокировки содержатся дополнительные блоки информации или интерактивных элементов, которые по умолчанию закомментированы. В режиме редактирования HTML-кода в шаблон блокировки можно добавить следующие сведения и формы:

- Поле для указания причины добавления URL в белый список.
- Дата блокировки.
- IP-адрес пользователя, отправившего запрос, который был заблокирован.
- Форма ввода логина и пароля администратора для снятия блокировки.

Чтобы создать пользовательский шаблон страницы блокировки:

1. В разделе **Настройки → Библиотеки → Шаблоны страниц** нажмите **Добавить** и выберите **Страница блокировки**.
2. Выберите из списка созданный шаблон и нажмите **Экспорт**. На ПК загрузится шаблон в формате HTML-страницы.
3. Используя текстовый редактор, откройте страницу, найдите закомментированные блоки для отображения дополнительных сведений и раскомментируйте нужные.

**Примечание** Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут изменить внутреннюю структуру шаблона.

4. Импортируйте измененную страницу в созданный шаблон.

## Настройка пользовательского оформления страниц

По умолчанию шаблоны страниц настроены на отображение сведений в стандартном оформлении. Вы можете использовать шаблоны в качестве основы для создания пользовательских шаблонов в собственном стиле, например в стиле вашей организации.

Чтобы настроить оформление страницы:

1. В разделе **Настройки → Библиотеки → Шаблоны страниц** нажмите **Добавить** и создайте шаблон страницы нужного типа.
2. Выберите из списка созданный шаблон и нажмите **Экспорт**. На ПК загрузится шаблон в формате HTML-страницы.
3. Используя текстовый редактор, откройте страницу и отредактируйте HTML-код для настройки собственного оформления.

**Примечание** Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут изменить внутреннюю структуру шаблона.

4. Импортируйте измененную страницу в созданный шаблон.

Категории URL

Version: 7.x  
Product: NGFW  
Documentation: 

Библиотека **Категории URL** содержит группы категорий UserGate URL Filtering, которые можно использовать в правилах фильтрации контента.

Для использования категорий UserGate URL Filtering требуется соответствующая лицензия.

Базовый набор категорий поставляется вместе с продуктом. При необходимости администратор может создавать дополнительные группы категорий и изменять их состав.

| Группа категорий                    | Описание                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threats                             | Набор категорий, рекомендованных для блокировки в целях обеспечения безопасности сети                                                                                                                                                                                                                                                                                 |
| Parental Control                    | Набор категорий, рекомендованных для блокировки в целях защиты детей от нежелательного контента                                                                                                                                                                                                                                                                       |
| Productivity                        | Набор категорий, рекомендованных для блокировки в целях повышения эффективности работы сотрудников                                                                                                                                                                                                                                                                    |
| Safe categories                     | Набор категорий, считаемых безопасными для посещения. Рекомендуется отключать морфологическую проверку, перехват HTTPS-трафика для данной группы категорий в целях уменьшения количества ложных срабатываний                                                                                                                                                          |
| Recommended for morphology checking | Набор категорий, рекомендованных для проверки с помощью морфологического анализа. Из этого набора исключены такие категории, как «Новости», «Финансы», «Правительство», «Информационная безопасность», «Детские сайты» и ряд других в целях уменьшения количества ложных срабатываний. Этот же набор категорий рекомендуется использовать для перехвата трафика HTTPS |
| Recommended for virus check         | Набор категорий, рекомендованных для антивирусной проверки                                                                                                                                                                                                                                                                                                            |

Для добавления новой группы категорий:

- Создайте группу категорий. В разделе **Настройки → Библиотеки → Категории URL** на панели **Группы URL категорий** нажмите **Добавить**, и укажите название группы.
- Добавьте в группу необходимые категории. Выделите созданную группу, в панели **Категории** нажмите **Добавить** и выберите необходимые категории из списка.

В системе определены следующие категории URL:

| ID | Уровень риска     | Название                                                | Описание                                                                                                                                                                                         |
|----|-------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0  | Высокий (4)       | Неизвестная тематика / Unknown                          | Сайты без принадлежности к какой-либо категории.                                                                                                                                                 |
| 1  | Высокий (4)       | Реклама и всплывающие окна / Advertisements and Pop-Ups | Сайты, содержащие графическую рекламу (баннеры, всплывающие окна и прочее).                                                                                                                      |
| 2  | Низкий (2)        | Алкоголь и табак / Alcohol and Tobacco                  | Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции                                                                                                  |
| 3  | Очень высокий (5) | Анонимайзеры / Anonymizers                              | Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхода средств веб-фильтрации и т.д.                        |
| 4  | Очень низкий (1)  | Искусство / Arts                                        | Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т.д.                                                                       |
| 5  | Очень низкий (1)  | Бизнес / Business                                       | К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах, необходимых предприятиям любого размера для успешной деятельности. |
| 6  | Очень низкий (1)  | Транспорт / Transportation                              | Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами, сообщества, клубы автолюбителей и т.д.                    |
| 7  | Средний (3)       | Чаты / Chat                                             | Сайты, позволяющие осуществлять общение в режиме реального времени.                                                                                                                              |

| ID | Уровень риска     | Название                                           | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----|-------------------|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8  | Очень низкий (1)  | Детские сайты / Kids sites                         | Сайты, ориентированные на детскую аудиторию                                                                                                                                                                                                                                                                                                                                                                                                         |
| 9  | Низкий (2)        | Форумы и новостные ленты / Forums and Newsgroups   | Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги.                                                                                                                                                                                                                                                                                                                                                          |
| 10 | Очень высокий (5) | Заражённые сайты / Compromised                     | Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ без ведома владельцев. В категорию также входят ресурсы из группы высокого риска заражения.                                                                                                                                                                                                                                                     |
| 11 | Очень низкий (1)  | Компьютеры и технологии / Computers and Technology | Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах.                                                                                                                                                                                                                                                                                     |
| 12 | Средний (3)       | Преступная деятельность / Criminal Activity        | Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения. |
| 13 | Средний (3)       | Сайты знакомств / Dating and Personals             | Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств, ресурсы, предлагающие эскорт-услуги.                                                                                                                                                                                                                                                             |
| 14 | Высокий (4)       | Download-архивы / Download Sites                   | Сайты, которые содержат доступное для скачивания программное обеспечение. Данная категория также включает в себя некоторые Peer-to-Peer сайты.                                                                                                                                                                                                                                                                                                      |
| 15 | Очень низкий (1)  | Образование / Education                            | Сайты, поддерживаемые учебными заведениями и школами всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы.                                                                                                                                                                                        |
| 16 | Низкий (2)        | Развлечения / Entertainment                        | Сайты, предлагающие пользователю телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости.                                                                                                                                                                                                                                                                    |
| 17 | Низкий (2)        | Финансы / Finance                                  | Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний, порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д.                                                                                                                                     |
| 18 | Высокий (4)       | Азартные игры / Gambling                           | Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами.                                                                                                                                                                                                                                                                                                                                                                 |
| 19 | Низкий (2)        | Игры / Games                                       | Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читках.                                                                                                                                                                                                                                                                                                                           |
| 20 | Очень низкий (1)  | Правительство / Government                         | Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц.                                                                                                                                                                                                       |
| 21 | Низкий (2)        | Ненависть и нетерпимость / Hate and Intolerance    | Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.                                                                                                                                                                                                                                                                       |
| 22 | Низкий (2)        | Здоровье и медицина / Health and Medicine          | Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной, рецептами лекарств, и т.д.                                                                                                                                                            |
| 23 | Низкий (2)        | Наркотики / Illegal Drug                           | Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами.                                                                                                                                                                                                                                                                              |
| 24 | Очень низкий (1)  | Поиск работы / Job Search                          | Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний.                                                                                                                                                                                                                                                                                    |
| 25 | Средний (3)       | Военные сайты / Military                           | Информация о военных организациях, военной истории.                                                                                                                                                                                                                                                                                                                                                                                                 |

| ID | Уровень риска     | Название                                                                | Описание                                                                                                                                                                                                                                                                                                                    |
|----|-------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26 | Высокий (4)       | Потоковое мультимедиа и загрузки / Streaming Media and Downloads        | Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.                                                                                                                    |
| 27 | Очень низкий (1)  | Новости / News                                                          | Новостные сайты: онлайн-журналы, новостные ленты и т.д.                                                                                                                                                                                                                                                                     |
| 28 | Низкий (2)        | Некоммерческие и неправительственные организации / Non-profits and NGOs | Сайты, посвященные клубам, сообществам, союзам и некоммерческим организациям. Значительное число данных структур созданы в образовательных или благотворительных целях.                                                                                                                                                     |
| 29 | Низкий (2)        | Нудизм / Nudity                                                         | Ресурсы, содержащие изображение частичной или полной наготы. Категория включает в себя сайты, рекламирующие или продающие нижнее белье, интимную одежду или купальные костюмы.                                                                                                                                              |
| 30 | Средний (3)       | Персональные сайты / Personal Sites                                     | Персональные сайты, созданные отдельными людьми или группами лиц, блоги.                                                                                                                                                                                                                                                    |
| 31 | Очень высокий (5) | Фишинг и мошенничество / Phishing and Fraud                             | Сайты, которые используются для обмана или в мошеннических целях (например, фишинг), такие как кражи финансовой или другой информации посредством учетной записи пользователя. Эти сайты чаще всего являются искусно выполненной подделкой популярных законных ресурсов, что вводит в заблуждение пользователей.            |
| 32 | Очень низкий (1)  | Политика / Politics                                                     | Сайты, посвященные политическим партиям или занимающиеся политической пропагандой, а также предоставляющие информацию о группах интересов, выборах, законодательстве или вопросе лоббирования. Категория включает в себя сайты, которые предлагают сведения о правах и их защите.                                           |
| 33 | Очень высокий (5) | Порнография и насилие / Pornography/Sexually Explicit                   | Сайты, которые содержат контент сексуального содержания. Категория включает в себя продукцию для взрослых, такую как секс-игрушки, компакт-диски и видео. Сайты из данной группы позволяют заказывать эскорт-услуги, получить сведения о стриптиз-клубах, почитать эротические рассказы и текстовые описания половых актов. |
| 34 | Низкий (2)        | Недвижимость / Real Estate                                              | Информация об аренде, покупке или продаже недвижимости или земельных участков. Рекомендации по покупке или продаже жилых помещений. Агентства недвижимости, услуги по аренде, переезду, улучшению жилищных условий.                                                                                                         |
| 35 | Низкий (2)        | Религия / Religion                                                      | Сайты, посвященные вопросу веры, человеческой духовности и религиозным убеждениям, в том числе сайты церквей, синагог, мечетей и других молитвенных домов.                                                                                                                                                                  |
| 36 | Очень низкий (1)  | Рестораны и еда / Restaurants and Dining                                | Сайты, содержащие списки, обзоры заведений общественного питания. Категория включает в себя сайты с рецептами, инструкциями и советами, продуктами питания и советами по выбору вина.                                                                                                                                       |
| 37 | Очень низкий (1)  | Поисковые системы и порталы / Search Engines and Portals                | Сайты, позволяющие осуществлять поиск в интернете по новостям, изображениям, каталогам и другим видам онлайн-контента. Категория включает в себя порталы и каталоги сайтов, такие как белые/желтые страницы.                                                                                                                |
| 38 | Низкий (2)        | Покупки / Shopping                                                      | Интернет-магазины, каталоги, аукционы, рекламные объявления. Категория не включает в себя ресурсы, посвященные товарам и услугам из более узких категорий, таких как здравоохранение и медицина.                                                                                                                            |
| 39 | Средний (3)       | Социальные сети / Social Networking                                     | Сайты социальных сетей, пользователи которых могут общаться, взаимодействовать, обмениваться сообщениями, файлами.                                                                                                                                                                                                          |
| 40 | Очень высокий (5) | Спам-сайты / Spam Sites                                                 | Сайты, продвижение которых основано на использовании спам-рассылок.                                                                                                                                                                                                                                                         |
| 41 | Очень низкий (1)  | Спорт / Sports                                                          | Сайты команд или спортивных ассоциаций, международные и национальные, спортивные колледжи. Ресурсы, содержащие результаты и расписания игр, спортивные журналы и газеты, виртуальный спорт и спортивные лиги.                                                                                                               |
| 42 | Очень высокий (5) | Вредоносное ПО / Malware                                                | Сайты, содержащие нежелательные программы, автоматически загружающиеся и устанавливающиеся на ПК пользователей. Вирусы вносят изменения в систему и позволяют злоумышленникам получить данные с компьютера без ведома и согласия его владельца.                                                                             |
| 43 | Низкий (2)        | Фондовый рынок / Stock trading                                          | Сайты по торговле ценными бумагами и управления инвестиционными активами. Также включает информацию о финансово-инвестиционной стратегии, котировкам и новостям.                                                                                                                                                            |
| 44 | Очень низкий (1)  | Переводчики / Translators                                               | Сайты, на которых возможен онлайн-перевод веб-страниц на другие языки. Данные ресурсы могут использоваться для обхода заданных ограничений, так как просмотр сайтов осуществляется с URL сайта онлайн-переводчика.                                                                                                          |

| ID | Уровень риска     | Название                                                                                   | Описание                                                                                                                                                                                                                                                 |
|----|-------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 45 | Очень низкий (1)  | Путешествия / Travel                                                                       | Авиакомпании, агентства по бронированию авиабилетов, планирование поездок, предварительные заказы, аренда транспортных средств, описания мест назначения, реклама гостиниц и казино.                                                                     |
| 46 | Низкий (2)        | Насилие / Violence                                                                         | Сайты, содержащие изображения, текстовые описания и пропаганду физического насилия против людей, животных или организаций\сообществ. Категория включает в себя ресурсы с иллюстрациями ужасов природы, а также сайты, содержащие ненормативную лексику.  |
| 47 | Низкий (2)        | Оружие / Weapons                                                                           | Сайты, содержащие изображения, обзоры и описания оружия. В категории также входят интернет-магазины орудий и оружия, в том числе для занятия спортом.                                                                                                    |
| 48 | Высокий (4)       | Веб-почта / Web-based Email                                                                | Порталы, позволяющие завести собственные почтовые аккаунты для написания, чтения, отправки и получения электронных писем.                                                                                                                                |
| 49 | Средний (3)       | Общие / General                                                                            | Сайты, которые не попадают в другие категории, например, пустые веб-страницы.                                                                                                                                                                            |
| 50 | Низкий (2)        | Отдых и оздоровление / Leisure and Recreation                                              | Сайты, связанные с рекреационной деятельностью и увлечениями, включая ресурсы, посвященные зоопаркам, центрам общественного отдыха, бассейнам, паркам развлечений и хобби, таким как садоводство, литература, искусства и ремесла, домашний декор и т.д. |
| 51 | Низкий (2)        | Онлайн обучение / Online training and tools                                                | Дистанционное образование, онлайн-курсы, профессиональное обучение, программы обучения, повышения квалификации.                                                                                                                                          |
| 52 | Низкий (2)        | Юриспруденция / Legal                                                                      | Сайты юридических фирм, обсуждение и анализ юридических вопросов.                                                                                                                                                                                        |
| 53 | Низкий (2)        | Местные достопримечательности / Local Information                                          | Путеводители и информация для туристов, в том числе о ресторанах и местные достопримечательности.                                                                                                                                                        |
| 54 | Низкий (2)        | Справочная информация / Reference and Research                                             | Профессиональные или образовательные справочные материалы, в том числе онлайн-словари, карты, переписи, альманахи, каталоги библиотек, генеалогии, и научной информации.                                                                                 |
| 55 | Очень низкий (1)  | Форумы с технической или бизнес информацией / Technical or business forums and news groups | Сайты с обсуждениями, относящимся к деловой или технической тематикам.                                                                                                                                                                                   |
| 56 | Очень низкий (1)  | Техническая информация / Technical information and documentation                           | Сайты, которые предоставляют информацию к технической документации и информации.                                                                                                                                                                         |
| 57 | Высокий (4)       | Персональные хранилища / Personal Storage                                                  | Сайты, которые позволяют загружать файлы и резервные копии для удаленного хранения данных.                                                                                                                                                               |
| 58 | Низкий (2)        | CDNs                                                                                       | Сети предоставления контента                                                                                                                                                                                                                             |
| 59 | Низкий (2)        | Нецензурная лексика / Profanity                                                            | Сайты, содержащие нецензурную лексику                                                                                                                                                                                                                    |
| 60 | Низкий (2)        | Профессиональные социальные сети / Professional social networks                            | Подмножество веб-сайтов социальных сетей, которое включает в себя контент, предназначенный исключительно для бизнеса и профессионалов.                                                                                                                   |
| 61 | Очень высокий (5) | Ботнеты / Botnets                                                                          | Сайты, которые управляют сетями ботов через командно-контрольные центры.                                                                                                                                                                                 |
| 62 | Низкий (2)        | Религиозные культы / Cults                                                                 | Сайты, связанные с нетрадиционной религиозной практикой, обычно называемой культами. Подобные движения считаются ложными, неортодоксальными, экстремистскими. Члены культов зачастую живут под руководством харизматического лидера.                     |
| 63 | Низкий (2)        | Мода и красота / Fashion and Beauty                                                        | Сайты о моде, ювелирных изделиях, гламуре, красоте, модельном бизнесе, косметике или связанных со всем перечисленным товарах или услугах. Включает отзывы, сравнения, а также общую информацию, полезную потребителю.                                    |

| ID | Уровень риска     | Название                                                         | Описание                                                                                                                                                                                                                                                                                                                                          |
|----|-------------------|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 64 | Низкий (2)        | Поздравительные открытки / Greeting cards                        | Сайты, которые позволяют людям получать и отправлять поздравительные открытки.                                                                                                                                                                                                                                                                    |
| 65 | Очень высокий (5) | Хакерство / Hacking                                              | Сайты, которые способствуют или содержат рекомендации о том, как получить несанкционированный доступ к компьютерным системам с целью кражи информации, совершения мошеннических действий, советы по созданию вирусов или совершению других видов незаконной деятельности, связанной с кражей цифровой информации.                                 |
| 66 | Очень высокий (5) | Криптомайнеры / Cryptocurrency Mining                            | Сайты, которые используют технологии майнинга криптовалют без разрешения пользователя.                                                                                                                                                                                                                                                            |
| 67 | Очень высокий (5) | Нелегальное ПО / Illegal Software                                | Сайты, которые незаконно распространяют программное обеспечение или защищенные авторским правом материалы, такие как фильмы, музыка, незаконные серийные номера, генераторы ключей.                                                                                                                                                               |
| 68 | Высокий (4)       | Обмен картинками / Image Sharing                                 | Порталы для размещения цифровых фотографий и изображений, фотоальбомы и фотообменники.                                                                                                                                                                                                                                                            |
| 69 | Низкий (2)        | Информационная безопасность / Information Security               | Сайты, которые предоставляют информацию о законной защите данных, в том числе о новых угрозах и способах борьбы с ними.                                                                                                                                                                                                                           |
| 70 | Средний (3)       | Сервисы мгновенных сообщений / Instant Messaging                 | Сайты, которые позволяют создавать и использовать аккаунт в службах обмена мгновенными сообщениями, таких как ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, и т.п.                                                                                                                                                               |
| 71 | Очень низкий (1)  | Сетевые ошибки / Network Errors                                  | Сайты, которым не присвоен IP-адрес.                                                                                                                                                                                                                                                                                                              |
| 72 | Средний (3)       | Паркованные домены / Parked Domains                              | К паркованным доменам относятся URL-адреса с ограниченным контентом, конечные точки перехода с рекламных объявлений. Подобные ресурсы могут приносить прибыль, но, как правило, не несут в себе полезной для пользователя информации. Категория также включает в себя сайты, находящиеся на реконструкции, папки и базовые страницы веб-серверов. |
| 73 | Высокий (4)       | Пиринговые сети / Peer-to-Peer                                   | Сайты, которые позволяют осуществлять прямой обмен файлами между пользователями вне зависимости от центрального сервера.                                                                                                                                                                                                                          |
| 74 | Высокий (4)       | Частные IP-адреса / Private IP Addresses                         | Включает наборы IP-адресов, определенные в RFC 1918.                                                                                                                                                                                                                                                                                              |
| 75 | Низкий (2)        | Школьные мошенничества / School Cheating                         | Сайты с ответами на различные школьные тесты, написанными эссе, рефератами, исследовательскими или курсовыми работами.                                                                                                                                                                                                                            |
| 76 | Низкий (2)        | Половое воспитание / Sex Education                               | Сайты, связанные с сексуальным образованием, включая такие темы, как уважение к партнеру, аборт, бисексуальный образ жизни, противозачаточные средства, заболевания, передаваемые половым путем и беременность.                                                                                                                                   |
| 77 | Средний (3)       | Сайты сомнительного содержания / Tasteless                       | Сайты с оскорбительным контентом, такого рода как юмор "ниже пояса", ужасный или даже пугающий контент, шокирующие изображения крови, ран или жестокого обращения с животными.                                                                                                                                                                    |
| 78 | Низкий (2)        | Жестокое обращение с детьми / Child Abuse Images                 | Сайты, содержащие фотографии, иллюстрирующие случаи жестокого обращения с детьми.                                                                                                                                                                                                                                                                 |
| 79 | Очень низкий (1)  | Нетрадиционная сексуальная ориентация / Gay, Lesbian or Bisexual | Сайты, содержащие материалы о геях, лесбиянках, трансгендерах.                                                                                                                                                                                                                                                                                    |
| 80 | Низкий (2)        | Литература и книги / Literature and Books                        | Сайты, содержащие опубликованные книги, новеллы, рассказы, включая фантастику, биографии.                                                                                                                                                                                                                                                         |
| 81 | Низкий (2)        | Здоровое питание и диеты / Nutrition and Diet                    | Сайты, посвященные правильному питанию, снижению веса, диетам.                                                                                                                                                                                                                                                                                    |
| 82 | Низкий (2)        | Домашние животные / Pets and Animals                             | Сайты, посвященные продуктам и сервисам для домашних и других животных.                                                                                                                                                                                                                                                                           |

| ID | Уровень риска     | Название                                                | Описание                                                                                                                                                               |
|----|-------------------|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 84 | Низкий (2)        | Обновления / Updates                                    | Сайты обновлений программного обеспечения, обновлений операционных систем, обновлений                                                                                  |
| 85 | Средний (3)       | Чат-боты<br>искусственного<br>интеллекта / Chat-bot AI  | Сайты, предоставляющие доступ к чат-ботам искусственного интеллекта, подобным Chat GPT.                                                                                |
| 97 | Низкий (2)        | Репутация: Низкий риск<br>/ Reputation: Low risk        | Сайты с низким репутационным риском. Как правило это сайты, не имеющие известных уязвимостей, но относящиеся к категориям, где риск нарушения безопасности возможен.   |
| 98 | Средний (3)       | Репутация: Средний<br>риск / Reputation:<br>Medium risk | Сайты со средним репутационным риском. Как правило это сайты, которые могут содержать уязвимости и относящиеся к категориям, где риск нарушения безопасности возможен. |
| 99 | Очень высокий (5) | Репутация: Высокий<br>риск / Reputation: High<br>risk   | Сайты с высоким репутационным риском. Сайты с известными уязвимостями.                                                                                                 |

## Измененные категории URL

---

Version: 7.x

Product: NGFW

Documentation: 

Библиотека **Измененные категории URL** предназначена для переопределения категорий сайтов. Назначенные пользователем категории имеют приоритет над категориями, определенными специалистами UserGate. Переопределение может потребоваться при ошибочной категоризации сайта или при отсутствии у него категории.

Для переопределения категории:

1. Проверьте категорию сайта. В разделе **Настройки → Библиотеки → Измененные категории URL** введите адрес сайта в строку проверки и нажмите **Проверить категорию**.
2. Если текущая категория не соответствует требуемой, нажмите **Добавить** и назначьте сайту до двух новых категорий.

После сохранения изменений сайт будет добавлен в список переопределений. Для каждой записи отображаются дата изменения, имя администратора, выполнившего изменение, исходные и назначенные категории.

При дальнейших проверках система будет возвращать категории, назначенные пользователем, а также специальную категорию **Переопределенные пользователем категории**.

Для массового назначения категорий сайтам можно импортировать список переопределений из файла в формате TXT и CSV.

Каждая строка файла должна содержать следующие поля, разделенные запятыми:

A,B,C,D,E

где:

- A — доменное имя сайта, для которого необходимо переопределить категорию;
- B — идентификатор назначаемой категории;
- C — идентификатор ранее определенной категории (опциональный информационный параметр); укажите 0, если категория ранее не была определена;
- D — временная метка в формате UTC Timestamp (получить значение можно [по ссылке](#));
- E — комментарий или описание (опциональный параметр).

Идентификаторы категорий URL можно посмотреть [по ссылке](#).

**Примечание** Удаление записи из библиотеки не приводит к восстановлению исходной категории сайта. Назначенная ранее измененная категория сохраняется.

Пример текстового файла импорта со списком переопределений:

```
test1test1.ru,69,0,Admin,1780368107,Тест 1
test2test2.ru,69,0,Admin,1780368108,Тест 2
test3test3.ru,69,0,Admin,1780368109,Тест 3
```

Technology: L7  
Version: 7.x  
Product: NGFW  
Documentation: ☒

Сигнатуры приложений представляют собой совокупность семантических выражений, с помощью которых описываются характерные признаки определенных сетевых приложений. Сигнатуры используются для анализа трафика на 7 уровне модели OSI.

Типы сигнатур приложений

В UserGate NGFW могут использоваться два типа сигнатур приложений:

- проприетарные;
- пользовательские.

Проприетарные сигнатуры приложений создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. В библиотеке приложений они помечаются выражением «@UserGate» в колонке **Владелец**.

Пользовательские сигнатуры приложений создаются самими пользователями. Для создания пользовательской сигнатуры в веб-консоли администратора необходимо перейти в раздел **Библиотеки → Приложения** и нажать **Добавить**. Далее необходимо задать параметры приложения и описать его признаки с помощью синтаксиса [UASL](#).

Параметры пользовательской сигнатуры приложения.

| Наименование   | Описание                                                                                                                                                                                                                                                                                               |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Тип            | Тип сигнатуры; <ul style="list-style-type: none"><li>• Приложение,</li><li>• Протокол,</li><li>• Поддержка — вспомогательная сигнатура.</li></ul>                                                                                                                                                      |
| Id             | Идентификатор сигнатуры. Если поле оставить пустым, то будет выдан свободный id из пользовательского пула.                                                                                                                                                                                             |
| Название       | Название сигнатуры.                                                                                                                                                                                                                                                                                    |
| Описание       | Описание сигнатуры.                                                                                                                                                                                                                                                                                    |
| Уровень угрозы | Уровень угрозы, определяемый сигнатурой. Определены следующие значения: <ul style="list-style-type: none"><li>• 1 — очень низкий;</li><li>• 2 — низкий;</li><li>• 3 — средний;</li><li>• 4 — высокий;</li><li>• 5 — очень высокий.</li></ul>                                                           |
| Технология     | Технология приложения: <ul style="list-style-type: none"><li>• <b>browser-based</b> — браузерное веб-приложение;</li><li>• <b>client-server</b> — клиент-серверное приложение;</li><li>• <b>network-protocol</b> — сетевой протокол;</li><li>• <b>peer-to-peer</b> — приложение точка-точка.</li></ul> |

| Наименование | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Категория    | <div>Категория сигнатуры приложений — группа сигнатур, объединенных общими параметрами. Список категорий приложений может быть пополнен.</div> <div><ul style="list-style-type: none"><li>Media streaming;</li><li>Email;</li><li>Coin Miners;</li><li>Tunneling;</li><li>Games;</li><li>Remote access;</li><li>Conferencing;</li><li>Trojan Horses;</li><li>Business;</li><li>Mobile;</li><li>Proxies and anonymizers;</li><li>Standard networks;</li><li>VOIP;</li><li>Web posting;</li><li>Software update;</li><li>File storage and backup;</li><li>Web browsing;</li><li>File sharing P2P;</li><li>Instant messaging</li><li>Social networking</li></ul></div> |
| UASL         | Описание признаков сигнатуры с помощью синтаксиса <a href="#">UASL</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

О создании сигнатур приложений в интерфейсе командной строки — в разделе «[Настройка библиотек](#)».

Сигнатуры приложений, зависимые от типа протокола

Для корректной работы некоторых сигнатур приложений в профилях необходимо наличие сигнатур определенного протокола.

В следующей таблице представлены такие зависимости.

| Сигнатура протокола | ID зависимых сигнатур                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSL/TLS (id=19)     | <div>185, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 198, 199, 200, 201, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 267, 268, 269, 270, 271, 272, 273, 275, 276, 277, 278, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 437, 439, 440, 441, 443, 444, 445, 446, 449, 450, 451, 458, 459, 465, 466, 470, 471, 472, 474, 475, 477, 481, 482, 485, 486, 487, 490, 492, 494, 495, 496, 501, 502, 504, 505, 511, 512, 513, 515, 516, 517, 518, 521, 524, 525, 526, 527, 528, 531, 532, 535, 536, 537, 538, 539, 544, 549, 550, 552, 554, 556, 557, 560, 563, 564, 566, 567, 568, 576, 577, 579, 581, 585, 589, 590, 592, 595, 596, 597, 600, 601, 603, 604, 606, 607, 610, 612, 613, 617, 621, 622, 623, 625, 627, 632, 635, 636, 638, 710, 730, 731, 734, 738, 739, 744, 746, 748, 752, 753, 754, 755, 756, 759, 760, 761, 762, 763, 766, 769, 770, 771, 772, 773, 774, 775, 776, 781, 783, 785, 788, 790, 795, 797, 800, 801, 807, 808, 810, 811, 813, 815, 817, 818, 820, 822, 825, 826, 831, 832, 833, 835, 836, 837, 841, 842, 846, 847, 848, 850, 851, 852, 853, 854, 858, 859, 860, 863, 864, 867, 869, 872, 874, 875, 877, 878, 879, 880, 883, 885, 887, 888, 891, 893, 894, 895, 897, 898, 899, 902, 903, 904, 905, 908, 909, 1967, 2027, 4062, 4082, 4437, 4459, 5294, 5301, 5317, 5321, 5323, 5324, 5385, 5395, 5407, 5431, 5506, 5637, 5641, 5644, 5645, 5649, 5650, 5652, 5654, 5656, 5658, 5668, 5671, 5673, 5674, 5675, 5676, 5678, 5679, 5680, 5681, 5688, 5692, 5693, 5695, 5699, 5710, 5711, 5715, 5719, 5730, 5736, 5739, 5740, 5742, 5744, 5750, 5762, 5765, 5769, 5770, 5773, 5776, 5777, 5778, 5786, 5791, 5792, 5794, 5795, 5800, 5804, 5809, 5810, 5812, 5813, 5815, 5816, 5820, 5822, 5823, 5825, 5826, 5827, 5828, 7688, 7689, 7690, 7691, 7692, 7694, 7695, 7698, 7699, 7704, 7705, 7707, 7708, 7740, 7843, 7864, 7865, 7867, 7868, 8000, 8001, 8002, 8003, 8004, 8005, 8006, 8007, 8009, 8010, 8011, 8012, 8014, 8015, 8016, 8017, 8018, 8019, 8022, 8024, 8026, 8027, 8028, 8031, 8032, 8033, 8034, 8035, 8036, 8037, 8038, 8039, 8040, 8041, 8043, 8044, 8045, 8048, 8049, 8053, 8054, 8055, 8056, 8057, 8058, 8059, 8060, 8063, 8064, 8066, 8067, 8069, 8070, 8071, 8075, 8077, 8078, 8079, 8080, 8081, 8082, 8083, 8084, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8094, 8095, 8096, 8098, 8099, 8101, 8102, 8103, 8104, 8105, 8106, 8107, 9003, 9007, 9008, 9016, 9019, 9030, 9042, 9044, 9048, 9050, 9051, 9052, 9053, 9054, 9055, 9056, 9057, 9058, 9059, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9068, 9069, 9071, 9072, 9074, 9075, 9076, 9077, 9078, 9079, 9080, 9081, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9090, 9091, 9092, 9094, 9096, 9097, 9098, 9099, 9100, 9101, 9102, 9103, 9104, 9105, 9114, 9128, 9141, 9147, 9148, 9150, 9529, 9543, 9544, 9553, 9563, 9566, 9572, 9573, 9575, 9579, 9580, 9622, 9625, 9627, 9628, 9641, 9650, 9655, 9657, 9714, 9733, 10514, 11011, 11024, 11025, 11044, 11504, 12001, 12002, 12003, 12006, 12007, 12008, 12009, 12010, 12011, 12012, 12013, 12014, 12015, 12016, 12017, 12018, 12019, 12020, 12021, 12022, 12023, 12024, 12025, 12026, 12027, 12028, 12033, 12034, 12035, 12036, 12044, 12045, 12501, 14002, 14003</div> |

| Сигнатура протокола | ID зависимых сигнатур                                                                                                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP (id=3)         | 196, 239, 261, 475, 532, 535, 610, 612, 627, 710, 1967, 4133, 4340, 4441, 5323, 5395, 5506, 5655, 5672, 5674, 5676, 5693, 5728, 5730, 5750, 5754, 5763, 5769, 5770, 5773, 5778, 5788, 5792, 5823, 5830, 7867, 8002, 8013, 8048, 9777, 9823, 9824, 9845, 11027, 12032, 12033 |
| DNS (id=5)          | 1967, 5395, 5672, 5815                                                                                                                                                                                                                                                      |
| IKE (id=11041)      | 11056                                                                                                                                                                                                                                                                       |

Связанные сигнатуры

Ряд сигнатур приложений зависят не только от сигнатур протокола, но и от других связанных сигнатур.

Список связанных сигнатур приложений приведен в следующей таблице.

| ID сигнатуры | Название сигнатуры   | Зависит от протокола | Связана с сигнатурой                             | Примечание                                                                                                                              |
|--------------|----------------------|----------------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 218          | Yandex.Disk          | SSL/TLS (id=19)      | —                                                | Для работы данной сигнатуры в профиль необходимо добавить только сигнатуру протокола (id=19).                                           |
| 7707         | Yandex.Disk download | SSL/TLS (id=19)      | Yandex.Disk (id=218), Yandex Services (id=12044) | Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанные сигнатуры (id=218 и id=12044). |
| 7708         | Yandex.Disk upload   | SSL/TLS (id=19)      | Yandex.Disk (id=218), Yandex Services (id=12044) | Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанные сигнатуры (id=218 и id=12044). |
| 12044        | Yandex Services      | SSL/TLS (id=19)      | —                                                | Для работы данной сигнатуры в профиль необходимо добавить только сигнатуру протокола (id=19).                                           |
| 16020        | Yandex Tracker       | SSL/TLS (id=19)      | Yandex Services (id=12044)                       | Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанную сигнатуру (id=12044).          |
| 12045        | Yandex Cloud         | SSL/TLS (id=19)      | Yandex Services (id=12044)                       | Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанную сигнатуру (id=12044).          |

Тайм-ауты приложений

В UserGate NGFW для приложений можно установить пользовательские значения тайм-аута бездействия ( idle timeout) — времени, в течение которого сессия будет сохраняться открытой, если в ней не производится обмен пакетами.

Значение тайм-аута по умолчанию для приложения зависит от протокола транспортного уровня, который использует приложение. Для TCP это значение равно 18 000 сек., для UDP — 60 сек.

Значение пользовательского тайм-аута можно установить в настройках сигнатуры приложения.

Пользовательский тайм-аут бездействия назначается на установившуюся сессию, как только сигнатура приложения определилась (сработала) в текущем трафике:

- Для протокола TCP — после того, как соединение переходит в состояние ESTABLISHED.
- Для протокола UDP — после того, как соединение переходит в состояние ASSURED. Состояние ASSURED возникает при обработке пакета (третьего по счету на соединении) после установки состояния REPLIED.

Значение пользовательского тайм-аута настраивается в интерфейсе командной строки (CLI) на уровне libraries application-signature. Подробнее — в разделе [Настройка библиотек](#).

Version: 7.x  
Technology: L7  
Product: NGFW  
Documentation: ☒

### Назначение профиля приложений

Профиль приложений позволяет создавать динамический набор [сигнатур приложений](#), предназначенный для анализа трафика на 7 уровне модели OSI. Динамичность профиля достигается за счет того, что профиль явно не содержит в себе никаких сигнатур, а содержит фильтры, с помощью которых собирается набор сигнатур. При изменении библиотеки сигнатур приложений профили динамически наберут новые наборы сигнатур, удовлетворяющих фильтрам профилей.

Помимо создания необходимого набора сигнатур в профиле могут определяться действия, которые необходимо выполнить над приложениями, отфильтрованными сигнатурами, и действия, которые должны быть применены к трафику, который не удалось идентифицировать.

### Создание профиля приложений в веб-консоли администратора

В веб-консоли администратора профили приложений создаются в разделе **Библиотеки → Профили приложений**.

В консоли администратора по умолчанию созданы два профиля приложений:

- Default application profile — профиль, содержащий все сигнатуры приложений, за исключением относящихся к категории ICS/IoT.
- Pass ICS/IoT applications — профиль, содержащий только сигнатуры приложений с категорией ICS/IoT (приложения, относящиеся к АСУ ТП).

Для создания собственного профиля необходимо нажать **Добавить** и заполнить соответствующие поля в свойствах профиля приложений:

1. В поле **Название** указать название создаваемого профиля.
2. В поле **Описание** опционально указать назначение профиля.
3. В области **Фильтры** добавляются фильтры для выбора необходимых сигнатур из библиотеки и настраиваются действия, которые необходимо выполнить над приложениями, отфильтрованными сигнатурами.
4. В области **Настройки сигнатуры неопределенных приложений** определяются действия с трафиком, который не был определен сигнатурами данного профиля.
5. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур приложений, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над приложениями, отфильтрованными этими сигнатурами.

### Настройка фильтров сигнатур в профиле приложений

Для создания фильтра сигнатур приложений необходимо в области **Фильтры** нажать **Добавить**. Откроется окно свойств фильтра.

Фильтр можно создать, выбирая опции отбора в панели инструментов. Ниже в окне будут отображаться сигнатуры из библиотеки, попадающие под действие этого фильтра:

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |

Также фильтр можно создать, описав его с помощью sql-подобного синтаксиса. Для этого необходимо нажать **Расширенный** в панели инструментов и в открывшейся строке описать свойства выбора фильтра:

|  |
|--|
|  |
|--|

В каждом фильтре могут настраиваться состояния сигнатур и действия, которые применяются ко всем сигнатурам, попадающим под него:

- включение/отключение сигнатуры;
- включение/отключение журналирования сигнатуры;
- запись в rсар-файл, если сигнатура сработала;
- предпринимаемое действие над трафиком, если сигнатура сработала, т.е. приложение было найдена в трафике; действия могут быть следующие: пропустить, отбросить, сбросить с разрывом TCP-соединения (reject), заблокировать IP-адрес источника или назначения.

Для сохранения созданного фильтра необходимо нажать **Сохранить**.

В одном профиле может быть создано сразу несколько фильтров.

Фильтры в профиле работают по правилу логического ИЛИ.

Порядок фильтров сигнатур в профиле важен - настройки верхнего фильтра имеют высший приоритет. Например, если в библиотеку сигнатур приложений будут добавлены новые сигнатуры и они попадут под действие сразу нескольких фильтров одного профиля, им будет присвоено настроенное действие первого фильтра, под который они попадают.

## Настройка действий для трафика, который не удалось идентифицировать

В профиле приложений может быть настроено действие, которое применяется к трафику, который не удалось идентифицировать с помощью набора сигнатур профиля.

В области **Настройки сигнатуры неопределенных приложений** настраивается действие, включается/отключается журналирование и запись в файл pcap.

Действия могут быть следующие: пропустить, отбросить, сбросить с разрывом TCP-соединения (reject).

Работа с профилями приложений в интерфейсе командной строки описана в разделе [Настройка библиотек](#) Руководства администратора.

## Примеры настроек профилей приложений

### Пример 1. Профиль приложения с сигнатурой, зависимой от сигнатуры протокола

Списки сигнатур, зависимых от сигнатур протоколов, приведены в разделе [Приложения](#).

Создадим профиль для приложения Kontur Talk, которое определяется соответствующей сигнатурой (id=14002). Чтобы запретить весь трафик, кроме трафика

приложения Kontur Talk, профиль приложений должен выглядеть следующим образом:



Сигнатура SSL/TLS (id=19) необходима для работы сигнатуры Kontur Talk, поэтому она добавляется в профиль, но для нее выставляется действие **Отбросить**, чтобы не пропускать посторонний трафик по протоколам SSL/TLS. Для неидентифицированного трафика также устанавливается действие **Отбросить**.

## Пример 2. Профиль для белого списка со связанными сигнатурами

Списки связанных сигнатур приведены в разделе [Приложения](#).

Создадим профиль для случая, когда необходимо разрешить загрузку файлов на Yandex Disk. Для того, чтобы сигнатура Yandex.Disk upload работала, необходимо учесть её зависимость от сигнатуры протокола SSL/TLS (id=19) и связанность с сигнатурами Yandex.Disk (id=218) и Yandex Services (id=12044). В данном примере профиль приложений будет выглядеть следующим образом:

Таким образом разрешается доступ и загрузка файлов на Yandex Disk, а весь остальной трафик помечается как неидентифицированный и отбрасывается либо действием сигнатуры SSL/TLS, либо действием для сигнатур неопределенных приложений.

### Пример 3. Профиль для черного списка со связанными сигнатурами

В данном примере разрешается весь трафик, кроме попадающего под сигнатуру Yandex.Disk upload (id=7708). Для этого случая необходимо учесть зависимость сигнатуры Yandex.Disk upload от сигнатуры протокола SSL/TLS (id=19). Связанность с сигнатурами Yandex.Disk и Yandex Services **в случае блокировки не учитывается**. Профиль приложений в данном примере будет выглядеть следующим образом:



Таким образом запрещается загрузка файлов на Yandex Disk, а весь остальной трафик разрешается либо действием сигнатуры SSL/TLS, либо действием для сигнатур неопределённых приложений.

## Применение профилей приложений

Администратор может создать необходимое количество профилей. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты определенного сервиса. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.

Профиль приложения применяется в разрешающем правиле [межсетевого экрана](#).

**Внимание!**Для корректной работы системы анализа трафика COB/L7 через NGFW должен проходить как прямой, так и обратный трафик. На асимметричном трафике система работать не будет.

Правила межсетевого экрана обрабатываются сверху вниз и сессия попадает в первое правило, которое удовлетворяет всем условиям в нем (адреса/зоны источника/назначения, пользователи итд.). После попадания под разрешающее правило с профилем приложений, трафик начинает анализироваться с помощью сигнатур профиля. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур профиля будет выполнено действие, настроенное в фильтрах профиля и произведена соответствующая запись в [Журнале трафика](#), если была включена опция журналирования. Если ни одна из сигнатур не была найдена, то к трафику будет применено действие, настроенное в профиле для неопределённых приложений.

**Примечание**При выбранном действии «Пропустить» для неопределённых приложений, попадающий под это условие, трафик будет безусловно разрешаться, не переходя дальше в обработку цепочки нижестоящих правил Межсетевого экрана.

Если срабатывает сигнатура с действием Блокировать IP, то тогда блокируется IP-адрес источника или назначения (в зависимости от настройки) на определенное в настройках время. Заблокированные сигнатурами IP-адреса отображаются на странице **Диагностика и мониторинг** в разделе **Заблокированные COB/L7 IP-адреса** (подробнее читайте в разделе [Заблокированные COB/L7 IP-адреса](#)).

## Виджеты сработавших приложений

Администратор может настроить отображение виджетов приложений на информационной панели — дашборде. В виджеты попадает информация о сработавших в правилах сигнатурах приложений, которые были определены в соответствующих профилях.

На NGFW предопределены 3 шаблона виджетов для приложений:

- Топ 10 приложений;
- Топ 10 разрешённых приложений;
- Топ 10 заблокированных приложений.

Виджеты можно добавлять на страницы дашборда и настраивать.

В настройках виджетов можно изменять:

- название;
- количество отображаемых записей;
- способ отображения информации (гистограмма или таблица);
- фильтр поиска информации для отображения;
- описание виджета.

Пример настройки виджета в шаблоне "Топ 10 разрешённых приложений":

Пример отображения настроенных виджетов приложений с гистограммами на дашборде:

Пример отображения настроенных виджетов приложений с таблицами на дашборде:

## Группы приложений

Version: 7.x  
Product: NGFW  
Documentation: 

В данном разделе пользователь может управлять (создавать/обновлять/удалять) группами приложений. Группы приложений могут быть использованы при настройке правил управления пропускной способности.

Для создания группы приложений:

| Наименование                                   | Описание                                                                                                                                                                                     |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Шаг 1. Создать группу.                         | В разделе <b>Библиотеки → Группы приложений</b> нажать на кнопку <b>Добавить</b> , указать название и, опционально, описание группы приложений.                                              |
| Шаг 2. Добавить сигнатуры приложений в группу. | На панели <b>Приложения</b> нажать <b>Добавить</b> и выбрать сигнатуры приложений для добавления в группу. Для добавления всех сигнатур приложений использовать кнопку <b>Добавить все</b> . |

Почтовые адреса

Version: 7.x  
Product: NGFW  
Documentation:

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

| Наименование                                     | Описание                                                                                                                            |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать группу почтовых адресов.   | В панели <b>Группы почтовых адресов</b> нажать на кнопку <b>Добавить</b> , дать название группе.                                    |
| <b>Шаг 2.</b> Добавить почтовые адреса в группу. | Выделить созданную группу, в панели <b>Почтовые адреса</b> нажать на кнопку <b>Добавить</b> и добавить необходимые почтовые адреса. |

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

| Наименование                                                                | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать файл с необходимыми списком почтовых адресов.         | Создать файл <b>list.txt</b> со списком почтовых адресов.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Шаг 2.</b> Создать архив, содержащий этот файл.                          | Поместить файл в архив zip с именем <b>list.zip</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Шаг 3.</b> Создать файл с версией списка.                                | Создать файл <b>version.txt</b> , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Шаг 4.</b> Разместить файлы на веб-сервере.                              | Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Шаг 5.</b> Создать список почтовых адресов и указать URL для обновления. | <p>На каждом NGFW создать список адресов. При создании указать тип списка <b>Обновляемый</b> и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:</p> <ul style="list-style-type: none"><li>Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.</li><li>Ежедневно.</li><li>Еженедельно.</li><li>Ежемесячно.</li><li>Каждые ... часов.</li><li>Каждые ... минут.</li><li>Задать вручную.</li></ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"><li>Звездочка (*) — обозначает весь диапазон (от первого до последнего).</li><li>Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.</li><li>Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li><li>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа".</li></ul> |

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

md5sum list.zip

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Номера телефонов

Documentation: ☒  
Product: NGFW  
Version: 7.x

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.  
Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

| Наименование                                      | Описание                                                                                                                             |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать группу телефонных номеров.  | В панели <b>Группы телефонных номеров</b> нажать на кнопку <b>Добавить</b> , дать название группе.                                   |
| <b>Шаг 2.</b> Добавить номера телефонов в группу. | Выделить созданную группу, в панели <b>Группа телефонных номеров</b> нажать на кнопку <b>Добавить</b> и добавить необходимые номера. |

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

| Наименование                                                                  | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Шаг 1.</b> Создать файл с необходимыми списком номеров.                    | Создать файл <b>list.txt</b> со списком номеров.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Шаг 2.</b> Создать архив, содержащий этот файл.                            | Поместить файл в архив zip с именем <b>list.zip</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Шаг 3.</b> Создать файл с версией списка.                                  | Создать файл <b>version.txt</b> , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Шаг 4.</b> Разместить файлы на веб-сервере.                                | Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Шаг 5.</b> Создать список телефонных номеров и указать URL для обновления. | <p>На каждом NGFW создать список адресов. При создании указать тип списка <b>Обновляемый</b> и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:</p> <ul style="list-style-type: none"><li>Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.</li><li>Ежедневно.</li><li>Еженедельно.</li><li>Ежемесячно.</li><li>Каждые ... часов.</li><li>Каждые ... минут.</li><li>Задать вручную.</li></ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"><li>Звездочка (*) — обозначает весь диапазон (от первого до последнего).</li><li>Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.</li><li>Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li><li>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "**/2" в поле "часы" будет означать "каждые два часа".</li></ul> |

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.  
Получить чек-сумму в linux можно командой:

md5sum list.zip

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

# Сигнатуры COB

Technology: IDPS  
Version: 7.x  
Product: NGFW

Сигнатуры COB представляют собой выражения на языке UASL и содержат описания паттернов (строк), которые COB распознает в сетевом трафике.

Для использования сигнатуры COB устройством необходимо [создать профиль COB](#), включающий эту сигнатуру, и добавить созданный профиль [в разрешающее правило межсетевого экрана](#).

Сигнатуры COB в UserGate NGFW делятся на пользовательские сигнатуры, которые вы можете [создавать в веб-консоли устройства](#), и проприетарные сигнатуры, разрабатываемые компанией UserGate и поставляемые [в рамках лицензии на модуль Security Updates](#).

Для проприетарных сигнатур вы можете настраивать [некоторые параметры](#) (например, изменять действие при срабатывании сигнатуры). Это может понадобиться для адаптации таких сигнатур под сетевую инфраструктуру организации. При необходимости вы можете восстановить исходные значения параметров проприетарных сигнатур, установленные экспертами UserGate.

## Просмотр списка сигнатур

В разделе **Настройки → Библиотеки → Сигнатуры COB** отображается список доступных сигнатур COB.

Для каждой сигнатуры в таблице отображаются следующие параметры.

| Параметр           | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Уровень угрозы     | Уровень опасности угрозы (от 1 до 5, где 1 — очень низкий уровень), который определяет степень потенциального ущерба ИТ-инфраструктуре при срабатывании сигнатуры                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Id                 | Идентификатор сигнатуры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Статус             | Статус параметров проприетарной сигнатуры: <ul style="list-style-type: none"><li>По умолчанию — значения параметров сигнатуры соответствуют значениям, установленным экспертами UserGate;</li><li>Изменено — значения параметров сигнатуры изменены администратором устройства</li></ul>                                                                                                                                                                                                                                                                                            |
| Журналирование     | Статус журналирования срабатываний сигнатуры: <ul style="list-style-type: none"><li>Журналируется — журналирование включено в свойствах сигнатуры, записи о ее срабатывании отображаются <a href="#">в Журнале COB</a>;</li><li>Не журналируется — журналирование отключено в свойствах сигнатуры</li></ul>                                                                                                                                                                                                                                                                         |
| Свойства сигнатуры | По нажатию на значок в столбце параметра открывается карточка выбранной сигнатуры                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Название сигнатуры | Название сигнатуры, указанное при ее создании                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Действие           | Действие при срабатывании сигнатуры: <ul style="list-style-type: none"><li>Нет — маркировка пакета или проверка наличия метки, установленной другой сигнатурой. Используется для сигнатур, связанных через конструкцию .mark set test. Подробнее — в разделе «<a href="#">Работа с метками</a>».</li><li>Пропустить — разрешение передачи трафика.</li><li>Отбросить — запрет передачи трафика.</li><li>Сбросить — запрет передачи трафика и разрыв TCP-соединения с его источником.</li><li>Блокировать IP — блокирование IP-адреса источника и (или) назначения трафика</li></ul> |

| Параметр                       | Описание                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Операционная система сигнатуры | Операционная система, для которой разработана сигнатура                                                                                                                                                                                                                                                                                                                              |
| Протокол                       | Сетевой протокол соединений, к которым применима сигнатура                                                                                                                                                                                                                                                                                                                           |
| Дата создания                  | Дата создания сигнатуры. Параметр доступен начиная с версии 7.5.0                                                                                                                                                                                                                                                                                                                    |
| Дата модификации               | Дата изменения сигнатуры. Параметр доступен начиная с версии 7.5.0                                                                                                                                                                                                                                                                                                                   |
| Класс                          | Класс сигнатуры, который определяет тип угрозы по срабатыванию этой сигнатуры. Ниже в этом разделе перечислены <a href="#">классы сигнатур в UserGate NGFW</a>                                                                                                                                                                                                                       |
| References                     | Идентификаторы уязвимости, на которую указывает срабатывание сигнатуры, согласно реестрам CVE и BDU                                                                                                                                                                                                                                                                                  |
| Категория                      | Категория сигнатуры, в которую объединяются сигнатуры с общими параметрам. Ниже в этом разделе перечислены <a href="#">категории сигнатур в UserGate NGFW</a>                                                                                                                                                                                                                        |
| PCAP включен                   | Запись копии трафика (трассировка) при срабатывании сигнатуры: <ul style="list-style-type: none"> <li><b>Включено</b> — трассировка выполняется, результат записывается в файл формата PCAP;</li> <li><b>Отключено</b> — трассировка не выполняется</li> </ul>                                                                                                                       |
| Владелец                       | Разработчик сигнатуры. Для проприетарных сигнатур отображается <b>UserGate</b> , для пользовательских — <b>You</b>                                                                                                                                                                                                                                                                   |
| Описание                       | Описание сигнатуры, указанное при ее создании.<br>Для проприетарных сигнатур отображается описание угрозы, на которую указывает срабатывание сигнатуры. Описание может включать сведения об уязвимостях в инфраструктуре организации, а также механику проведения и последствия атаки, использующей эти уязвимости.<br>По умолчанию в таблице сигнатур столбец <b>Описание</b> скрыт |

В таблице сигнатур вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки).

Кроме того, вы можете фильтровать данные в таблице, выбрав один из следующих режимов:

- **Простой** — с помощью доступных параметров. Например, фильтрация по состоянию сигнатур ( **true** — включено, **false** — отключено), уровню опасности угрозы, действию при срабатывании, а также владельцу сигнатур. Для выбора параметров используются соответствующие кнопки в панели инструментов. В раскрывающемся списке по кнопке **Еще** вы также можете выбирать дополнительные параметры фильтрации, устанавливая соответствующие флажки.
- **Расширенный** — с помощью специальных запросов [на языке фильтрации](#). Для ввода запросов используется строка фильтрации.

Вы можете управлять сигнатурами в таблице:

- Включать и отключать их состояние (по кнопкам **Включить** и **Отключить** соответственно).
- Создавать пользовательские сигнатуры (по кнопке **Добавить**).
- Изменять параметры сигнатур (по кнопке **Редактировать**). После изменения параметров проприетарных сигнатур вы можете восстановить значения этих параметров, установленные по умолчанию (по кнопке **Восстановить по умолчанию**).
- Просматривать информацию о сигнатуре в ее карточке (по нажатию на значок в столбце **Свойства сигнатуры** для выбранной сигнатуры).

## Создание пользовательской сигнатуры

**Примечание**Ниже приведена инструкция по созданию пользовательской сигнатуры в веб-консоли UserGate NGFW, аналогичная инструкция для интерфейса командной строки устройства приведена в разделе «[Настройка библиотек](#)».

Чтобы создать сигнатуру:

1. В разделе **Настройки** → **Библиотеки** → **Сигнатуры СОВ** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующие действия:
  - Активируйте сигнатуру, установив флажок **Включено**.
  - Если необходимо, укажите идентификатор сигнатуры, выбрав одно из доступных значений. При незаполненном поле идентификатор будет сгенерирован автоматически.
  - Укажите название и при необходимости описание сигнатуры.

- Выберите уровень опасности угрозы по срабатыванию сигнатуры (от 1 до 5, где 1 — очень низкий уровень).
- При необходимости выберите класс сигнатуры, определяющий тип угрозы по срабатыванию этой сигнатуры. Ниже в этом разделе перечислены [классы сигнатур в UserGate NGFW](#).
- При необходимости выберите категорию сигнатуры, в которую объединяются сигнатуры с общими параметрами. Ниже в этом разделе перечислены [категории сигнатур в UserGate NGFW](#).
- При необходимости укажите ОС, для которой создается сигнатура. Вы можете выбрать несколько значений.
- При необходимости укажите идентификатор уязвимости, на которую указывает срабатывание сигнатуры, согласно реестру CVE.
- При необходимости укажите идентификатор уязвимости, на которую указывает срабатывание сигнатуры, согласно реестру BDU.
- При необходимости укажите адрес ресурса с описанием уязвимости, на которую указывает срабатывание сигнатуры, в формате `https://<адрес ресурса>`, например `https://example.com`.

3. На вкладке **UASL и настройки** выполните следующие действия:

- В поле **UASL** укажите параметры сигнатуры [с помощью синтаксиса UASL](#).
- Выберите действие, выполняемое при срабатывании сигнатуры.  
Для сигнатуры с действием **Нет** вы можете указывать параметры только в поле **UASL**, остальные поля недоступны для настройки.
- Если не требуется записывать информацию о срабатываниях сигнатуры [в Журнал СОВ](#), отключите журналирование. По умолчанию журналирование включено.
- Если при срабатывании сигнатуры требуется сохранять копию трафика в виде файла формата PCAP, включите трассировку трафика в поле **Файл PCAP**. По умолчанию трассировка отключена.
- Для сигнатуры с действием **Сбросить** или **Блокировать IP** выберите направление трафика, к которому будет применяться сигнатура:
  - **Источник** — от клиента к серверу;
  - **Назначение** — от сервера к клиенту;
  - **Оба** — в обоих направлениях.
- Для сигнатуры с действием **Блокировать IP** выберите режим блокировки IP-адресов при срабатывании сигнатуры:
  - **Всегда** — постоянная блокировка;
  - **На время** — блокировка в течение указанного времени.

4. Нажмите **Проверить сигнатуру** для проверки синтаксиса UASL.

Результат проверки отобразится в отдельном окне.

5. Нажмите **Заккрыть**.

6. Если в синтаксисе UASL содержатся ошибки, исправьте их и повторите проверку.

7. Нажмите **Сохранить**.

## Настройка проприетарной сигнатуры

Чтобы настроить проприетарную сигнатуру:

1. Выберите сигнатуру в таблице и нажмите **Редактировать**.
2. Настройте параметры сигнатуры:
  - Состояние сигнатуры.
  - Действие, выполняемое при срабатывании.
  - Журналирование срабатываний.
  - Трассировку трафика при срабатывании.
  - Направление трафика, к которому применяется сигнатура. Доступно только для действий **Сбросить** и **Блокировать IP**.
  - Время блокировки IP-адресов при срабатывании. Доступно только для действия **Блокировать IP**. Для постоянной блокировки необходимо установить значение 0.

В некоторых проприетарных сигнатурах указаны параметры агрегации (суммирования) срабатываний этих сигнатур:

- **Частота срабатывания** — количество срабатываний сигнатуры за указанный период времени (в секундах). Например, если указано «5 срабатываний за 10 секунд», UserGate NGFW пропустит первые четыре срабатывания сигнатуры и выполнит выбранное действие только при пятом срабатывании.
- **Направление** — направление агрегирования срабатываний сигнатуры:
  - **IP источника** — суммируются срабатывания сигнатуры для каждого уникального IP-адреса клиента (источника трафика).
  - **IP назначения** — суммируются срабатывания сигнатуры для каждого уникального IP-адреса сервера (назначения трафика).

При необходимости вы можете изменить параметры агрегации. Это может понадобиться для снижения количества ложных срабатываний сигнатур, которые обнаруживают массовые атаки, например такие, как брутфорс (см. сигнатуру с id = 17002) или DoS (см. сигнатуру с id = 3040443).

3. Нажмите **Сохранить**.

## Классы сигнатур в UserGate NGFW

Сигнатуры СОВ в UserGate NGFW классифицируются по типу угрозы, на которую указывают их срабатывания (например, запуск произвольного кода, сетевая разведка или атака на веб-приложение). Эта классификация определяет, как именно срабатывание сигнатуры влияет на ИТ-инфраструктуру, и позволяет

администраторам эффективно управлять безопасностью.

В таблице ниже перечислены классы, используемые в проприетарных сигнатурах UserGate. При создании пользовательских сигнатур вы можете использовать только основные классы из этого перечня.

| Класс сигнатуры                 | Описание угрозы                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------|
| <b>arbitrary-code-execution</b> | Попытка выполнения произвольного кода                                                 |
| <b>arbitrary file access</b>    | Попытка доступа к произвольным файлам                                                 |
| <b>attempted-admin</b>          | Попытка получения прав администратора                                                 |
| <b>attempted-dos</b>            | Попытка DoS-атаки                                                                     |
| <b>attempted-recon</b>          | Попытка сетевой разведки                                                              |
| <b>attempted-user</b>           | Попытка получения прав пользователя                                                   |
| <b>authentication bypass</b>    | Попытка обхода аутентификации                                                         |
| <b>backdoor</b>                 | Обход стандартных механизмов аутентификации                                           |
| <b>bad-unknown</b>              | Потенциально вредоносный трафик                                                       |
| <b>bruteforce</b>               | Атака брутфорс                                                                        |
| <b>buffer overflow</b>          | Атака через переполнение буфера                                                       |
| <b>c2-activity</b>              | Активность, указывающая на подключение к командному центру злоумышленника             |
| <b>code injection</b>           | Попытка внедрения кода                                                                |
| <b>command injection</b>        | Попытка внедрения системных команд                                                    |
| <b>command-and-control</b>      | Попытка подключения к командному центру злоумышленника                                |
| <b>csrf</b>                     | Попытка выполнения несанкционированных действий от имени авторизованного пользователя |
| <b>default-login-attempt</b>    | Попытка входа с учетными данными по умолчанию                                         |
| <b>denial-of-service</b>        | DoS-атака                                                                             |
| <b>deserialization</b>          | Попытка удаленного выполнения кода (RCE), связанного с десериализацией параметров     |
| <b>evasion</b>                  | Попытка обхода злоумышленником механизмов защиты COB                                  |
| <b>exploit-kit</b>              | Использование злоумышленником набора инструментов для эксплуатации уязвимостей        |
| <b>file transfer</b>            | Попытка передачи файлов определенных типов                                            |
| <b>hardcoded credentials</b>    | Попытка использования злоумышленником встроенных учетных данных                       |
| <b>information disclosure</b>   | Попытка получения конфиденциальных данных                                             |
| <b>local file inclusion</b>     | Попытка доступа к локальным файлам сервера                                            |
| <b>memory corruption</b>        | Попытка атаки через повреждение памяти                                                |
| <b>misc</b>                     | Активность, не относящаяся к другим классам                                           |
| <b>misc activity</b>            | Потенциально опасная или опасная активность, не относящаяся к другим классам          |

| Класс сигнатуры                           | Описание угрозы                                                      |
|-------------------------------------------|----------------------------------------------------------------------|
|                                           |                                                                      |
| <b>misc attack</b> и <b>misc-attack</b>   | Попытка атаки, не относящейся к другим классам                       |
| <b>misc scan</b>                          | Попытка сканирования сети и поиска уязвимостей                       |
| <b>network scan</b> и <b>network-scan</b> | Сканирование сети на наличие активных узлов и открытых портов        |
| <b>null pointer dereference</b>           | Попытка атаки через ошибки обращения к памяти                        |
| <b>out of bounds access</b>               | Попытка атаки через переполнение или чтение памяти                   |
| <b>path traversal</b>                     | Попытка атаки через обход пути к файлам на сервере                   |
| <b>policy-violation</b>                   | Нарушение сетевых политик                                            |
| <b>privilege escalation</b>               | Попытка повышения привилегий                                         |
| <b>protocol-command</b>                   | Попытка использования нестандартных или вредоносных команд протокола |
| <b>protocol-command-decode</b>            | Попытка использования команд протокола в закодированном виде         |
| <b>remote file inclusion</b>              | Попытка удаленного внедрения файлов                                  |
| <b>service scan</b>                       | Попытка сканирования сетевых сервисов и их версий                    |
| <b>shellcode</b>                          | Попытка передачи шелл-кода для получения управления системой         |
| <b>shellcode-detect</b>                   | Попытка использования исполняемого кода (шелл-кода)                  |
| <b>sql injection</b>                      | Попытка SQL-внедрения                                                |
| <b>ssrf</b>                               | Попытка подделки запросов на стороне сервера                         |
| <b>string-detect</b>                      | Использование подозрительных строк                                   |
| <b>successful-recon-limited</b>           | Сетевая разведка ограниченного масштаба                              |
| <b>suspicious-filename-detect</b>         | Использование подозрительного имени файла                            |
| <b>suspicious-login</b>                   | Попытка входа с использованием подозрительного имени пользователя    |
| <b>system-call-detect</b>                 | Попытка использования системных вызовов                              |
| <b>targeted-activity</b>                  | Активность, указывающая на проведение целенаправленной атаки         |
| <b>trojan</b>                             | Активность, указывающая на работу вредоносного ПО                    |
| <b>trojan-activity</b>                    | Использование вредоносного ПО                                        |
| <b>uncaught exception</b>                 | Попытка вызова программных ошибок                                    |
| <b>uncontrolled resource consumption</b>  | Попытка исчерпания системных ресурсов                                |
| <b>use after free</b>                     | Попытка обращения к освобожденным участкам памяти                    |
| <b>vulnerability scan</b>                 | Сканирование сети на наличие уязвимостей                             |

| Класс сигнатуры          | Описание угрозы                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------|
| web-application-activity | Активность, связанная с работой веб-приложений                                             |
| web-application-attack   | Атака через уязвимости веб-приложений                                                      |
| worm                     | Активность, указывающая на работу самораспространяющегося вредоносного ПО (сетевого червя) |
| xml injection            | Попытка XML-внедрения                                                                      |
| xss                      | Попытка внедрения вредоносного сценария в веб-приложение                                   |

Список классов сигнатур постоянно пополняется экспертами UserGate.

### Категории сигнатур в UserGate NGFW

В UserGate NGFW сигнатуры с общими параметрами объединяются в категории по их функциональному назначению.

В таблице ниже перечислены категории, используемые в проприетарных сигнатурах UserGate. При создании пользовательских сигнатур вы можете использовать только основные категории из этого перечня.

| Категория сигнатур              | Функциональное назначение                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| activex                         | Защита от использования уязвимостей ActiveX                                                                         |
| adware pup                      | Поиск рекламного и нежелательного ПО                                                                                |
| attack response                 | Выявление в ответах сервера признаков проведенных атак                                                              |
| authentication-failures         | Обнаружение подбора учетных данных                                                                                  |
| authentication-failures,Apache  | Обнаружение подбора учетных данных к веб-серверу Apache                                                             |
| authentication-failures,ICS/IoT | Обнаружение подбора учетных данных в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT) |
| broken-access-control           | Выявление обхода прав доступа                                                                                       |
| broken-access-control,ICS/IoT   | Выявление обхода прав доступа в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)      |
| bruteforce                      | Обнаружение брутфорса                                                                                               |
| coinminer                       | Выявление скрытого майнинга                                                                                         |
| dns                             | Обнаружение угроз в трафике DNS                                                                                     |
| dos                             | Обнаружение DoS-атак                                                                                                |
| dos,Apache                      | Обнаружение DoS-атак на веб-сервер Apache                                                                           |
| dos,ICS/IoT (или ICS/IoT,dos)   | Обнаружение DoS-атак на промышленные системы управления (ICS) и устройства интернета вещей (IoT)                    |
| dos,smtp                        | Обнаружение DoS-атак на почтовые серверы                                                                            |
| exploit                         | Обнаружение использования известных уязвимостей                                                                     |
| exploit kit                     | Выявление наборов инструментов для эксплуатации уязвимостей                                                         |
| ftp                             | Обнаружение угроз в трафике FTP                                                                                     |
| icmp                            | Обнаружение угроз в трафике ICMP                                                                                    |

| Категория сигнатур                  | Функциональное назначение                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>ICS/IoT</b>                      | Обнаружение угроз в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)                         |
| <b>imap</b>                         | Обнаружение угроз в трафике IMAP                                                                                           |
| <b>info</b>                         | Выявление утечки конфиденциальных данных                                                                                   |
| <b>injection</b>                    | Обнаружение внедрения данных                                                                                               |
| <b>injection,Apache</b>             | Обнаружение внедрения данных на стороне веб-сервера Apache                                                                 |
| <b>injection,ftp</b>                | Обнаружение внедрения данных в трафике FTP                                                                                 |
| <b>injection,ICS/IoT</b>            | Обнаружение внедрения данных в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)              |
| <b>injection,scan</b>               | Выявление сканирования сети на наличие уязвимостей, используемых для внедрения данных                                      |
| <b>injection,smb</b>                | Обнаружение внедрения данных в трафике SMB                                                                                 |
| <b>injection,smtp</b>               | Обнаружение внедрения данных в трафике SMTP                                                                                |
| <b>integrity-failures</b>           | Выявление нарушений целостности данных или ПО                                                                              |
| <b>integrity-failures,Apache</b>    | Выявление нарушений целостности данных или конфигурации веб-сервера Apache                                                 |
| <b>integrity-failures,ICS/IoT</b>   | Выявление нарушений целостности данных или ПО в промышленных системах управления (ICS) и устройствах интернета вещей (IoT) |
| <b>integrity-failures,injection</b> | Обнаружение внедрений, нарушающих целостность данных или ПО                                                                |
| <b>ldap</b>                         | Обнаружение угроз в трафике LDAP                                                                                           |
| <b>malware</b>                      | Обнаружение вредоносного ПО                                                                                                |
| <b>malware,wmi</b>                  | Обнаружение вредоносной активности, использующей инструменты WMI                                                           |
| <b>misc</b>                         | Обнаружение прочих угроз                                                                                                   |
| <b>misc,ICS/IoT</b>                 | Обнаружение прочих угроз в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)                  |
| <b>misc,smtp</b>                    | Обнаружение прочих угроз в трафике SMTP                                                                                    |
| <b>netbios</b>                      | Обнаружение угроз в трафике NetBIOS                                                                                        |
| <b>p2p</b>                          | Обнаружение активности пиринговых сетей и протоколов                                                                       |
| <b>phishing</b>                     | Обнаружение активности, связанной с фишингом                                                                               |
| <b>policy</b>                       | Выявление нарушения политик безопасности                                                                                   |
| <b>pop3</b>                         | Обнаружение угроз в трафике POP3                                                                                           |
| <b>request-forgery</b>              | Обнаружение подделки запросов                                                                                              |
| <b>request-forgery,ICS/IoT</b>      | Обнаружение подделки запросов в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)             |
| <b>rpc</b>                          | Обнаружение угроз в трафике RPC                                                                                            |
| <b>scada</b>                        | Обнаружение угроз в трафике систем управления SCADA                                                                        |

| Категория сигнатур       | Функциональное назначение                                            |
|--------------------------|----------------------------------------------------------------------|
| <b>scan</b>              | Обнаружение активности по сканированию сети и поиску уязвимостей     |
| <b>shellcode</b>         | Обнаружение внедрения шелл-кода                                      |
| <b>sip</b>               | Обнаружение угроз в трафике SIP                                      |
| <b>smb</b>               | Обнаружение угроз в трафике SMB                                      |
| <b>smtp</b>              | Обнаружение угроз в трафике SMTP                                     |
| <b>snmp</b>              | Обнаружение угроз в трафике SNMP                                     |
| <b>sql</b>               | Обнаружение угроз в трафике баз данных                               |
| <b>telnet</b>            | Обнаружение угроз в трафике Telnet                                   |
| <b>tftp</b>              | Обнаружение угроз в трафике TFTP                                     |
| <b>user agents</b>       | Выявление подозрительных идентификаторов браузеров и приложений      |
| <b>voip</b>              | Обнаружение угроз в трафике протоколов IP-телефонии (VoIP)           |
| <b>web client</b>        | Обнаружение атак на веб-браузеры и клиентские приложения             |
| <b>web server</b>        | Обнаружение атак на веб-серверы и серверные приложения               |
| <b>web specific apps</b> | Обнаружение атак на веб-приложения                                   |
| <b>worm</b>              | Обнаружение самораспространяющегося вредоносного ПО (сетевых червей) |

Список категорий сигнатур постоянно пополняется экспертами UserGate.

Technology: IDPS

Version: 7.x

Product: NGFW

Documentation: 

### Назначение профиля COB

С помощью профилей COB администратор может создать динамические наборы [сигнатур COB](#), предназначенные для обнаружения вторжений и защиты определенных сервисов. Динамичность профилей достигается за счет использования фильтров, с помощью которых автоматически собирается необходимый набор сигнатур. Для фильтрации используются как описательные поля, так и параметры сигнатур. При изменении сигнатур в библиотеке профили динамически обновят наборы сигнатур в соответствии с настроенными фильтрами.

В профилях COB также можно настроить действия, которые будут выполняться над трафиком, отфильтрованным сигнатурами.

### Создание профиля COB в веб-консоли администратора

В веб-консоли администратора профили COB создаются в разделе **Настройки → Библиотеки → Профили COB**.

Нажмите **Добавить** и заполните соответствующие поля в свойствах профиля:

1. В поле **Название** укажите название создаваемого профиля.
2. В поле **Описание** укажите назначение профиля.
3. В области **Фильтры** добавьте фильтры для выбора необходимых сигнатур из библиотеки.
4. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур COB, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над трафиком, отфильтрованным этими сигнатурами.

### Настройка фильтров сигнатур в профиле COB

Для создания фильтра сигнатур в области **Фильтры** нажмите **Добавить**. Откроется окно свойств фильтра.

Фильтр можно создать, выбирая опции фильтрации в панели инструментов. В окне под панелью инструментов будут отображаться сигнатуры, отбираемые этим фильтром:

Также фильтр можно создать, описав его с помощью sql-подобного синтаксиса. Для этого нажмите **Расширенный** в панели инструментов и в открывшейся строке опишите свойства выбора фильтра:

Начиная с версии ПО 7.3.0 в свойствах фильтров доступна возможность перенастройки параметров всех сигнатур, отбираемых фильтром:



Вы можете перенастроить следующие параметры отфильтрованных сигнатур:

- **Состояние сигнатуры** — возможность включить или выключить сигнатуры. Значение «По умолчанию» оставляет состояние всех сигнатур таким, как было определено в самих сигнатурах по умолчанию.
- **Действие** — предпринимаемое действие, если сигнатура сработала, т. е. была найдена в трафике. Действия могут быть следующие: пропустить пакет, отбросить пакет, сбросить пакет с разрывом TCP-соединения, блокировать IP-адрес источника или назначения. Значение «По умолчанию» оставляет для всех сигнатур то действие, которое было определено в самих сигнатурах по умолчанию.
- **Журналировать** — включение или отключение журналирования срабатывания сигнатуры. Значение «По умолчанию» оставляет настройку журналирования для всех сигнатур, как она была определена в самих сигнатурах по умолчанию.
- **Файл PCAP** — включение или отключение записи в PCAP-файл, если сигнатура сработала. Значение «По умолчанию» оставляет настройку записи в PCAP-файл для всех сигнатур, как она была определена в самих сигнатурах по умолчанию.
- **Применить к** — настраивается, если параметр «Действие» выставлен в значения «Сбросить» или «Блокировать IP». Параметр имеет следующие значения:
  - Источник;
  - Назначение;
  - Оба.
- **Продолжительность** — можно настроить, если параметр «Действие» имеет значение «Блокировать IP». Число, указывающее срок блокировки IP-адреса. Если значение равно нулю, IP-адрес блокируется бесконечно.

Для сохранения созданного фильтра нажмите **Сохранить**.

В одном профиле можно использовать сразу несколько фильтров.

Фильтры в профиле работают по логическому ИЛИ. Например, если в профиле добавлено два фильтра: `category = injection` и `threat = low`, они эквивалентны одному фильтру: `category = injection OR threat = low`.

Если одна и та же сигнатура попала в несколько фильтров, приоритет настроек параметров сигнатуры определяется настройками в верхнем фильтре в списке.

Фильтры в профиле можно перемещать вверх или вниз:

### Точечное переопределение параметров сигнатур в профиле COB

На вкладке профиля **Совпавшие сигнатуры** можно произвести точечное переопределение параметров сигнатуры. Для этого выберите нужные сигнатуры в списке совпавших сигнатур и нажмите **Переопределить** в панели инструментов.



Переопределение настроек сигнатур в профиле COB имеет более высокий приоритет, чем настройки этих же сигнатур в библиотеке сигнатур COB.

Измененные настройки сигнатур COB можно вернуть в первоначальное состояние, для этого выделите сигнатуру в списке сигнатур профиля и нажмите в панели инструментов профиля **Восстановить по умолчанию**.



## Приоритет значений параметров сигнатуры COB

Приоритет назначений параметров сигнатуры COB определяется согласно следующей диаграмме:

- В библиотеке сигнатур COB (**Настройки** → **Библиотеки** → **Сигнатуры COB**) представлен общий перечень сигнатур с определенными по умолчанию параметрами. Администратор может [самостоятельно переопределить](#) некоторые параметры (например, состояние, действие, журналирование, запись в файл PCAP и т. д.) в настройках параметров сигнатуры.
- При создании профиля COB администратор может [переопределить параметры](#) сигнатур при настройке конкретного фильтра. Эти изменения будут актуальны только для профиля, в котором они определены.
- При создании профиля COB администратор может точно переопределить параметры сигнатур в списке всех совпавших сигнатур профиля (подробнее — в главе «[Точечное переопределение параметров сигнатур в профиле COB](#)»). Изменения применяются к результату фильтрации. Изменения параметров сигнатуры при точечном переопределении сохраняются до тех пор, пока сигнатура попадает в профиль.

**Примечание** Если в фильтре профиля задан поиск по свойствам сигнатур, этот поиск будет осуществляться с учетом свойств, заданных в библиотеке сигнатур («Настройки» → «Библиотеки» → «Сигнатуры COB»). Переопределения на этапе задания свойств фильтра, а также точечные переопределения на факт попадания сигнатуры в фильтр не влияют.

## Применение профилей COB

Администратор может создать необходимое количество профилей. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты определенного сервиса. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.

Профиль COB применяется в разрешающем правиле [межсетевого экрана](#).

Правила межсетевого экрана обрабатываются сверху вниз и сессия попадает в первое правило, которое удовлетворяет всем условиям в нем. После попадания под правило с профилем COB, трафик начинает анализироваться с помощью определенного в профиле набора сигнатур. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур профиля будет выполнено действие, настроенное в профиле и произведена соответствующая запись в [Журнале COB](#), если была включена опция журналирования. Если ни одна из сигнатур профиля не была найдена, то трафик пропускается дальше.

**Важно!** Для корректной работы системы анализа трафика COB/L7 через NGFW должен проходить как прямой, так и обратный трафик. На асимметричном трафике система работать не будет.

Если срабатывает сигнатура с действием Блокировать IP, то тогда блокируется IP-адрес источника или назначения (в зависимости от настройки) на определенное в настройках время. Заблокированные сигнатурами IP-адреса отображаются на странице **Диагностика и мониторинг** в разделе **Заблокированные COB/L7 IP-адреса** (подробнее читайте в разделе [Заблокированные COB/L7 IP-адреса](#)).

Работа с сигнатурами COB в интерфейсе командной строки описана в разделе [Настройка библиотек](#) Руководства администратора.

Профили оповещений

Version: 7.x  
Product: NGFW  
Documentation: 

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail.
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

| Наименование | Описание                                                                                                                                                                                |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название     | Название профиля.                                                                                                                                                                       |
| Описание     | Описание профиля.                                                                                                                                                                       |
| Хост         | IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.                                                                                            |
| Порт         | Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера. |
| Безопасность | Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.                                                                                                            |
| Авторизация  | Включает авторизацию при подключении к SMTP-серверу.                                                                                                                                    |
| Логин        | Имя учетной записи для подключения к SMTP-серверу.                                                                                                                                      |
| Пароль       | Пароль учетной записи для подключения к SMTP-серверу.                                                                                                                                   |

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

| Наименование               | Описание                                                                                                                                                                                                                                                                         |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название                   | Название профиля.                                                                                                                                                                                                                                                                |
| Описание                   | Описание профиля.                                                                                                                                                                                                                                                                |
| Хост                       | IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS сообщений.                                                                                                                                                                                          |
| Порт                       | Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL -- 3550.                                                                                                                                                   |
| SSL                        | Использовать или нет шифрацию с помощью SSL.                                                                                                                                                                                                                                     |
| Логин                      | Имя учетной записи для подключения к SMPP-серверу.                                                                                                                                                                                                                               |
| Пароль                     | Пароль учетной записи для подключения к SMPP-серверу.                                                                                                                                                                                                                            |
| Правила трансляции номеров | В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8. |

Профили Netflow

Version: 7.x  
Product: NGFW  
Documentation: 

Netflow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу Netflow требуются следующие компоненты:

- Сенсор — собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор — получает от сенсора данные и помещает их в хранилище.
- Аналитатор — анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты (часто в виде графиков).

NGFW может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс NGFW, необходимо выполнить следующие действия:

1. Создать профиль Netflow.
2. Назначить созданный профиль Netflow сетевому интерфейсу, на котором необходимо собирать статистику.

Для создания профиля Netflow необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили Netflow** и указать необходимые параметры:

| Наименование                           | Описание                                                                                                                                                                                                                                                                                             |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название                               | Название профиля Netflow.                                                                                                                                                                                                                                                                            |
| Описание                               | Описание профиля Netflow.                                                                                                                                                                                                                                                                            |
| IP-адрес Netflow коллектора            | IP-адрес сервера, куда сенсор будет отправлять статистику.                                                                                                                                                                                                                                           |
| Порт Netflow коллектора                | UDP порт, на котором коллектор будет принимать статистику.                                                                                                                                                                                                                                           |
| Версия протокола                       | Версия протокола Netflow, которую следует использовать. Версия протокола должна совпадать на сенсоре и на коллекторе.                                                                                                                                                                                |
| Таймаут активного потока (сек)         | При длительных потоках, например, передача большого файла через сеть, время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока. Значение по умолчанию — 1800 секунд.                                                                                          |
| Таймаут неактивного потока (сек.)      | Время, резервируемое на завершение неактивного потока. Значение по умолчанию — 15 секунд.                                                                                                                                                                                                            |
| Количество потоков                     | Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. Ограничение необходимо для защиты от DoS-атак. После достижения данного количества потоков, все последующие не будут учитываться. Значение по умолчанию — 2000000, установите 0 для снятия ограничения. |
| Отправлять информацию NAT              | Отправлять информацию о NAT преобразованиях в статистику Netflow.                                                                                                                                                                                                                                    |
| Частота отправки шаблона (пакетов)     | Количество пакетов, после которых шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.                                                             |
| Период отправки старого шаблона (сек.) | Время, через которое старый шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.                                                                  |

# Профили LLDP

Version: 7.x  
Product: NGFW  
Documentation: 

**Link Layer Discovery Protocol** (LLDP) — протокол канального уровня, позволяющий сетевым устройствам, работающим в локальной сети, объявлять о своём существовании и передавать свои характеристики и получать аналогичные сведения. Информация, собранная при помощи операции LLDP, хранится в сетевом устройстве.

Для создания профиля безопасности необходимо нажать **Добавить** в разделе **Библиотеки → Профили LLDP** и указать следующие параметры:

| Наименование | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название     | Название профиля LLDP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Описание     | Описание профиля LLDP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Статус порта | Режим: <ul style="list-style-type: none"><li>• <b>Приём и передача данных LLDP</b> — NGFW будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей.</li><li>• <b>Только приём данных LLDP</b> — NGFW не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей.</li><li>• <b>Только передача данных LLDP</b> — NGFW будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей.</li></ul> |

Профили SSL

Product: NGFW  
Version: 7.x  
Documentation: 

Профиль SSL позволяет указать протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи, которые в дальнейшем могут быть использованы в правилах инспектирования SSL, в настройках веб-консоли, страницы авторизации, страницы блокировки, веб-портале.

Для создания профиля SSL необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили SSL** и указать необходимые параметры:

| Наименование                 | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название                     | Название профиля SSL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Описание                     | Описание профиля SSL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Протоколы SSL                | <p><b>Минимальная версия TLS</b> — устанавливает минимальную версию TLS, которая может быть использована в данном профиле.</p> <p><b>Максимальная версия TLS</b> — устанавливает максимальную версию TLS, которая может быть использована в данном профиле.</p> <p>Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Наборы алгоритмов шифрования | <p>Данный раздел позволяет выбрать необходимые алгоритмы шифрования и цифровой подписи. Возможные значения указаны в виде строк, в которых перечислены алгоритм и подпись. Администратор может указать только те наборы алгоритмов и подписей, которые считает нужным для безопасной работы организации. Список поддерживаемых комбинаций следующий:</p> <ul style="list-style-type: none"><li>• TLS AES 128 CCM SHA256</li><li>• TLS AES 128 GCM SHA256</li><li>• TLS AES 256 GCM SHA384</li><li>• TLS DHE DSS WITH 3DES EDE CBC SHA</li><li>• TLS DHE DSS WITH AES 128 CBC SHA</li><li>• TLS DHE DSS WITH AES 128 CBC SHA256</li><li>• TLS DHE DSS WITH AES 128 GCM SHA256</li><li>• TLS DHE DSS WITH AES 256 CBC SHA</li><li>• TLS DHE DSS WITH AES 256 CBC SHA256</li><li>• TLS DHE DSS WITH AES 256 GCM SHA384</li><li>• TLS DHE RSA WITH 3DES EDE CBC SHA</li><li>• TLS DHE RSA WITH AES 128 CBC SHA</li><li>• TLS DHE RSA WITH AES 128 CBC SHA256</li><li>• TLS DHE RSA WITH AES 128 GCM SHA256</li><li>• TLS DHE RSA WITH AES 256 CBC SHA</li><li>• TLS DHE RSA WITH AES 256 CBC SHA256</li><li>• TLS DHE RSA WITH AES 256 GCM SHA384</li><li>• TLS ECDH ECDSA WITH 3DES EDE CBC SHA</li><li>• TLS ECDH ECDSA WITH AES 128 CBC SHA</li><li>• TLS ECDH ECDSA WITH AES 128 CBC SHA256</li><li>• TLS ECDH ECDSA WITH AES 128 GCM SHA256</li><li>• TLS ECDH ECDSA WITH AES 256 CBC SHA</li><li>• TLS ECDH ECDSA WITH AES 256 CBC SHA384</li><li>• TLS ECDH ECDSA WITH AES 256 GCM SHA384</li><li>• TLS ECDH RSA WITH 3DES EDE CBC SHA</li><li>• TLS ECDH RSA WITH AES 128 CBC SHA</li><li>• TLS ECDH RSA WITH AES 128 CBC SHA256</li><li>• TLS ECDH RSA WITH AES 128 GCM SHA256</li><li>• TLS ECDH RSA WITH AES 256 CBC SHA</li><li>• TLS ECDH RSA WITH AES 256 CBC SHA384</li><li>• TLS ECDH RSA WITH AES 256 GCM SHA384</li><li>• TLS ECDHE ECDSA WITH 3DES EDE CBC SHA</li><li>• TLS ECDHE ECDSA WITH AES 128 CBC SHA</li></ul> |

| Наименование                                                      | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                   | <ul style="list-style-type: none"> <li>• TLS ECDHE ECDSA WITH AES 128 CBC SHA256</li> <li>• TLS ECDHE ECDSA WITH AES 128 GCM SHA256</li> <li>• TLS ECDHE ECDSA WITH AES 256 CBC SHA</li> <li>• TLS ECDHE ECDSA WITH AES 256 CBC SHA384</li> <li>• TLS ECDHE ECDSA WITH AES 256 GCM SHA384</li> <li>• TLS ECDHE RSA WITH 3DES EDE CBC SHA</li> <li>• TLS ECDHE RSA WITH AES 128 CBC SHA</li> <li>• TLS ECDHE RSA WITH AES 128 CBC SHA256</li> <li>• TLS ECDHE RSA WITH AES 128 GCM SHA256</li> <li>• TLS ECDHE RSA WITH AES 256 CBC SHA</li> <li>• TLS ECDHE RSA WITH AES 256 CBC SHA384</li> <li>• TLS ECDHE RSA WITH AES 256 GCM SHA384</li> <li>• TLS GOST2012256 WITH 28147 CNT IMIT</li> <li>• TLS GOSTR341001 WITH 28147 CNT IMIT</li> <li>• TLS RSA WITH 3DES EDE CBC SHA</li> <li>• TLS RSA WITH AES 128 CBC SHA</li> <li>• TLS RSA WITH AES 128 CBC SHA256</li> <li>• TLS RSA WITH AES 128 GCM SHA256</li> <li>• TLS RSA WITH AES 256 CBC SHA</li> <li>• TLS RSA WITH AES 256 CBC SHA256</li> <li>• TLS RSA WITH AES 256 GCM SHA384</li> </ul> |
| <b>Установка алгоритмов шифрования для стандартных протоколов</b> | <p>Данный раздел можно использовать для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS. Администратор может указать в поле <b>Выберите протокол для установки алгоритмов</b> необходимые версии протоколов TLS, нажать на кнопку <b>Применить</b>, и алгоритмы, соответствующие выбранной версии протокола автоматически будут отмечены. Можно последовательно добавить несколько версий протокола TLS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

По умолчанию в продукте создано несколько профилей SSL, которые могут быть использованы администратором как есть, либо изменены/удалены при необходимости. Созданы следующие профили SSL:

| Наименование                             | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default SSL profile</b>               | <p>Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.1 до TLS v.1.2. Это наиболее распространенные версии протоколов, используемые в сети интернет в данное время. Данный профиль используется по умолчанию в:</p> <ul style="list-style-type: none"> <li>• Правилах инспектирования трафика SSL.</li> <li>• Для страницы авторизации Captive-портала.</li> <li>• Для страницы блокировки.</li> <li>• В веб-портале.</li> </ul> |
| <b>Default SSL profile (TLSv1.3)</b>     | Содержит алгоритмы и подписи, соответствующие версии TLS v.1.3. По умолчанию не используется.                                                                                                                                                                                                                                                                                                                                                 |
| <b>Default SSL profile (GOST)</b>        | Содержит алгоритмы и подписи, соответствующие TLS с ГОСТ-алгоритмами (TLS GOST2012256 with 28147 CNT IMIT и TLS GOSTR341001 with 28147 CNT IMIT). Может быть использован в организациях, где требуется использование данных алгоритмов, например, для веб-портала. Поддержка данных протоколов должна также быть обеспечена со стороны используемых браузеров. По умолчанию не используется.                                                  |
| <b>Default SSL profile (web console)</b> | <p>Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.0 до TLS v.1.2. Данный профиль используется по умолчанию для предоставления SSL-доступа в веб-консоль.</p> <p><b>Важно!</b> Изменение данного профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа в веб-консоль!</p>                                                                      |

Профили пересылки SSL

Version: 7.x  
Product: NGFW  
Documentation: 

Профили пересылки SSL работают совместно с правилами инспектирования SSL и позволяют указать устройства, на которые необходимо отправить копию расшифрованного трафика. Копия трафика будет отправлена в случае успешной расшифровки передаваемого трафика в соответствии с правилом инспектирования и выбранным профилем SSL.

Для создания профиля пересылки необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили пересылки SSL** и указать необходимые параметры:

| Наименование            | Описание                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название                | Название профиля пересылки SSL.                                                                                                                                                                                                                                                                                                                                                 |
| Описание                | Описание профиля пересылки SSL.                                                                                                                                                                                                                                                                                                                                                 |
| Тип пересылки           | Доступные типы пересылки: <ul style="list-style-type: none"><li>• <b>L2</b>. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика.</li><li>• <b>L3</b> туннель: копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адреса источника и назначения.</li></ul> |
| MAC-адрес назначения    | MAC-адрес устройства, на которое необходимо переслать копию расшифрованного трафика. Параметр указывается при выборе типа пересылки L2.                                                                                                                                                                                                                                         |
| Пересылать на интерфейс | Название интерфейса, на который необходимо пересылать копию расшифрованного трафика. Параметр указывается при выборе типа пересылки L2.                                                                                                                                                                                                                                         |
| GRE IP-адрес источника  | IP-адрес источника туннеля GRE. Параметр указывается при выборе типа пересылки L3.                                                                                                                                                                                                                                                                                              |
| GRE IP-адрес назначения | IP-адрес назначения туннеля GRE. Параметр указывается при выборе типа пересылки L3.                                                                                                                                                                                                                                                                                             |

НІР объекты

Version: 7.x  
Product: NGFW  
Documentation: 

Объекты НІР позволяют настроить критерии соответствия для конечных устройств и могут быть использованы в качестве одного из условий при настройке политик безопасности.

**Примечание**После подключения к NGFW конечное устройство будет отправлять телеметрию с периодичностью в 1 минуту.  
**Примечание**Для указания некоторых условий требуется наличие лицензированного модуля *Security Updates*, необходимого для скачивания обновлений библиотек.

Для добавления объекта необходимо указать:

| Наименование           | Описание                                                                                                                                                                                                                                                                                            |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название               | Название объекта НІР.                                                                                                                                                                                                                                                                               |
| Описание               | Описание объекта НІР (опционально).                                                                                                                                                                                                                                                                 |
| Версия ОС              | Версия операционной системы устройства пользователя.<br>При использовании операторов = и != необходимо указывать полную версию Windows.                                                                                                                                                             |
| Версия UserGate Client | Версия ПО UserGate Client.                                                                                                                                                                                                                                                                          |
| Безопасность           | Статусы компонентов безопасности конечного устройства: <ul style="list-style-type: none"><li>• Межсетевой экран;</li><li>• Антивирус;</li><li>• Автоматическое обновление;</li><li>• BitLocker.</li></ul> <b>Важно!</b> BitLocker считается включенным, если он включен хотя бы на одном из дисков. |

| Наименование             | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Продукты                 | <p>Проверка соответствия программного обеспечения, установленного на конечном устройстве:</p> <ul style="list-style-type: none"> <li>• <b>Антивирус.</b> Проверка соответствия антивирусного ПО на устройстве пользователя. <ul style="list-style-type: none"> <li>◦ <b>Включено:</b> проверка статуса ПО (да, нет, не проверять);</li> <li>◦ <b>Базы антивируса обновлены:</b> проверка актуальности баз (да, нет, не проверять) — производится только в случае, когда в предыдущем пункте включена проверка статуса антивируса в явном виде;</li> <li>◦ <b>Версия ПО;</b></li> <li>◦ <b>Вендор:</b> производитель и название продукта.</li> </ul> </li> <li>• <b>Межсетевой экран.</b> Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать: <ul style="list-style-type: none"> <li>◦ <b>Установлен:</b> проверка наличия установленного ПО;</li> <li>◦ <b>Включено:</b> проверка статуса ПО (да, нет, не проверять);</li> <li>◦ <b>Версия ПО;</b></li> <li>◦ <b>Вендор:</b> производитель и название продукта;</li> </ul> </li> <li>• <b>Резервное копирование.</b> Проверка ПО для резервного копирования: <ul style="list-style-type: none"> <li>◦ <b>Установлен:</b> проверка наличия установленного ПО;</li> <li>◦ <b>Версия ПО;</b></li> <li>◦ <b>Вендор:</b> производитель и название продукта.</li> </ul> </li> <li>• <b>Шифрование диска.</b> Проверка установленных на конечном устройстве программ для шифрования диска: <ul style="list-style-type: none"> <li>◦ <b>Установлен:</b> проверка наличия установленного ПО;</li> <li>◦ <b>Версия ПО;</b></li> <li>◦ <b>Вендор:</b> производитель и название продукта.</li> </ul> </li> <li>• <b>DLP.</b> Проверка соответствия системы предотвращения утечек информации. <ul style="list-style-type: none"> <li>◦ <b>Установлен:</b> проверка наличия установленного ПО;</li> <li>◦ <b>Версия ПО;</b></li> <li>◦ <b>Вендор:</b> производитель и название продукта.</li> </ul> </li> <li>• <b>Управление обновлениями.</b> Проверка актуальности обновлений. <ul style="list-style-type: none"> <li>◦ <b>Установлен:</b> проверка наличия установленного ПО;</li> <li>◦ <b>Версия ПО;</b></li> <li>◦ <b>Вендор:</b> производитель и название продукта.</li> </ul> </li> </ul> |
| Процессы                 | Проверка процессов, запущенных на конечном устройстве.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Запущенные службы        | Проверка служб, запущенных на конечном устройстве.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Ключи реестра            | <p>Ключ реестра Microsoft Windows - каталог, в котором хранятся настройки и параметры операционной системы.</p> <p>Поддерживаются следующие типы параметров реестра:</p> <ul style="list-style-type: none"> <li>• <b>REG_SZ:</b> строка Unicode или ANSI с нулевым символом в конце.</li> <li>• <b>REG_BINARY:</b> двоичные данные в любой форме.</li> <li>• <b>REG_DWORD:</b> 32-разрядное число.</li> </ul> <p>Доступна проверка ключей следующих разделов реестра:</p> <ul style="list-style-type: none"> <li>• <b>HKEY_LOCAL_MACHINE</b></li> <li>• <b>HKEY_USERS</b></li> </ul> <p><b>Важно!</b> Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру.</p> <p>Описание ключей реестра читайте в документации Microsoft ( <a href="https://docs.microsoft.com/ru-ru/troubleshoot/developer/webapps/iis/general/use-registry-keys">https://docs.microsoft.com/ru-ru/troubleshoot/developer/webapps/iis/general/use-registry-keys</a>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Установленные обновления | Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

# НІР-профилі

Version: 7.x  
Product: NGFW  
Documentation: 

Host Information Profile (HIP) позволяет производить сбор и анализ информации о степени защиты конечного устройства с установленным ПО UserGate Client. HIP профили представляют собой набор объектов HIP и предназначены для проверки соответствия конечного устройства требованиям безопасности (комплаенса). С использованием профилей HIP можно настроить гибкие политики доступа к зоне сети или приложению.

**Примечание**Для проверки комплаенса и работы правил межсетевого экрана, в которых в качестве одного из условий указан профиль HIP, необходимо наличие лицензии на модуль *Контроль доступа в сеть на уровне МЭ*.

При создании профиля необходимо указать:

| Наименование | Описание                                                                                                                                                                                                                                                                                        |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Включено     | Включение/отключение использования профиля.<br>Если профиль используется в правилах межсетевого экрана, то в случае его выключения, он будет помечен серым цветом.<br><b>Важно!</b> В случае выключения профиля правило межсетевого экрана продолжает работать без условия проверки комплаенса. |
| Название     | Название профиля HIP.                                                                                                                                                                                                                                                                           |
| Описание     | Описание профиля HIP (опционально).                                                                                                                                                                                                                                                             |
| Объекты HIP  | Выбор логического элемента (И, ИЛИ, И НЕ, ИЛИ НЕ) и объектов HIP.<br>Подробнее о создании объектов читайте в разделе <a href="#">Объекты HIP</a> .                                                                                                                                              |

**Примечание**Максимальное количество одновременно активных профилей не может превышать 32.

Профили BFD

Version: 7.x  
Product: NGFW  
Documentation: 

BFD (Bidirectional Forwarding Detection) — протокол, работающий на уровне интерфейса и протокола маршрутизации и предназначенный для быстрого обнаружения сбоев между двумя соседними маршрутизаторами, включая интерфейсы, каналы передачи данных и механизмы пересылки.

BFD работает поверх любого протокола передачи данных (сетевой уровень, канальный уровень, туннели и т.д.), передаваемого между двумя системами. Пакеты BFD передаются в качестве полезной нагрузки инкапсулирующего протокола, который подходит для данной среды и сети. BFD может работать на нескольких уровнях в системе.

Маршрутизаторы с BFD отправляют пакеты друг другу с согласованной скоростью. Если пакеты от маршрутизатора, поддерживающего BFD, не поступают, то этот маршрутизатор объявляется неработающим. BFD передает эту информацию соответствующим протоколам маршрутизации, и информация о маршрутизации обновляется. BFD помогает обнаружить односторонний отказ устройства и используется для быстрой конвергенции протоколов маршрутизации.

Профиль BFD — это конфигурация или набор параметров, используемых в протоколах динамической маршрутизации (BGP, OSPF), для определения работы функции обнаружения двунаправленной переадресации. Профиль обычно включает такие параметры, как желаемое время обнаружения, время удержания и другие параметры, определяющие скорость обнаружения и реагирования сетевых устройств на сбой в канале связи.

Настройка и использование профилей обеспечивают оперативное обнаружение сбоев в сети, что позволяет ускорить перенаправление трафика на интерфейсы и повысить надежность сети.

Настройка BFD для OSPF позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса OSPF.

В случае протокола BGP, BFD также может быть использован для регулирования времени обнаружения сбоев. Настройка BFD на более быстрое обнаружение неисправностей соединений позволяет оперативней реагировать и улучшать конвергенцию маршрутизации BGP.

Чтобы создать профиль BFD, необходимо в разделе **Библиотеки → Профили BFD** нажать **Добавить** и указать необходимые параметры:

| Наименование         | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Название             | Название профиля BFD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Описание             | Оptionальное описание профиля.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Определить множитель | <p>Множитель времени обнаружения. Локальная система рассчитывает время обнаружения неисправностей соединения как произведение множителя времени обнаружения, полученного от удалённой системы, и согласованного интервала передачи удалённой системы. Если BFD не получит управляющий пакет до истечения времени обнаружения, то считается, что произошел сбой соединения.</p> <p>Например, если интервал передачи равен 300 мс, а множитель — 3, то локальная система будет обнаруживать сбой только через 900 мс отсутствия приёма пакетов.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Интервал приёма      | <p>Интервал приёма управляющих пакетов BFD (минимальное время, которое требуется между пакетами). Для определения интервала каждый из узлов сравнивает свой интервал передачи с интервалом приема соседа — большее из двух значений принимается в качестве интервала передачи для этого узла.</p> <p>Значение по умолчанию — 50 мс.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Интервал передачи    | <p>Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами.</p> <p>Значение по умолчанию — 50 мс.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Время получения echo | <p>Минимальный интервал, через который система способна принимать echo-пакеты.</p> <p>Значение по умолчанию — 50 мс.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Время отправки echo  | <p>Минимальный интервал передачи, через который система будет способна отправлять echo-пакеты BFD.</p> <p>Значение по умолчанию — 50 мс.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Echo режим           | <p>Включение/отключение режима передачи Echo. По умолчанию этот режим отключён.</p> <p>Когда функция Echo активна, поток пакетов BFD Echo передается на удалённую систему, которая возвращает их обратно по тому же маршруту пересылки. Если некоторое количество пакетов Echo-потока данных не получено, сессия объявляется нерабочей.</p> <p>Echo-пакеты отличаются от control-пакетов (обычный режим) тем, что пакеты имеют адрес назначения равный адресу источника. Попадая на соседнюю систему, они проходят весь обычный транзитный путь, обеспечивая таким образом более полное тестирование работоспособности системы соседа. Учитывая специфику обработки и фильтрации пакетов в UserGate NGFW, для работы Echo-режима BFD необходимо создавать правило межсетевого экрана с разрешением соответствующего сервиса, иначе Echo-режим работать не будет. Например, для работы в Echo-режиме с Cisco IOS нужно создать сервис с разрешением UDP src port 49152 и dst port 3785.</p> |

| Наименование                   | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Пассивный режим</b>         | <p>Включение/отключение пассивного режима.</p> <p>При работе в пассивном режиме система ждёт управляющие пакеты от соседей и отвечает на них в случае их получения.</p> <p>Эта функция полезна, когда маршрутизатор выступает в роли центрального узла звездообразной сети, и требуется избежать отправки ненужных управляющих пакетов BFD.</p> <p>По умолчанию используется активный режим.</p> <p>При работе в активном режиме узел отправляет управляющие пакеты соседнему узлу.</p> <p>Оба узла не могут работать в пассивном режиме; хотя бы один из них (или оба) должны работать в активном режиме.</p> |
| <b>Минимальное время жизни</b> | <p>Только для сеансов с несколькими переходами.</p> <p>Настройка минимального значения времени жизни (количество переходов), которое BFD будет принимать в управляющем пакете BFD. Может принимать значения от 1 до 254. Все пакеты с меньшим значением TTL будут отброшены.</p> <p>Установка данного значения необходима для ужесточения требований к проверке пакетов во избежание получения управляющих пакетов BFD от других сессий.</p> <p>Значение по умолчанию равно 254 (это означает, что ожидается только один переход между этой системой и аналогом).</p>                                          |

## Syslog-фильтры UserID агента

Technology: Identification and Authentication  
Version: 7.x  
Product: NGFW  
Documentation: ☒

При использовании syslog в качестве источников событий UserGate производит фильтрацию событий в соответствии с указанными syslog-фильтрами UserID агента. Syslog-фильтры представляют собой стандартные регулярные выражения (regex), которые пользователь может писать самостоятельно.

**Примечание**Из-за особенностей работы устройств UserGate при создании регулярного выражения для поиска символа «\», который в regex также является символом для экранирования, следует указывать четыре символа «\\» подряд. Например: &user [A-Za-z0-9.-]\\\\([A-Za-z0-9.-])[&|@]?.

В стандартной поставке представлены три вида фильтров:

| Наименование            | Описание                                                                                                                                                               |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSH Authentication      | Фильтр, предназначенный для отслеживания событий входа или выхода пользователей по протоколу SSH в журналах syslog                                                     |
| Unix PAM Authentication | Фильтр, предназначенный для отслеживания событий входа или выхода пользователей посредством технологии <b>Pluggable Authentication Modules</b> (PAM) в журналах syslog |
| UserGate WEC Agent      | Фильтр, предназначенный для отслеживания событий, переданных через syslog из UserID агента для AD/WEC-серверов.<br>(Доступно начиная с релиза ПО 7.2.0)                |

**Примечание**С помощью regex вы также можете написать собственные фильтры. Таким образом фильтры syslog представляют из себя универсальный инструмент, который можно использовать практически в любых случаях.

Найденные события отображаются во вкладке **Журналы и отчёты**, в разделе **Журналы —> Агент UserID —> Syslog**.

Version: 7.x  
Product: NGFW

### Для чего нужны сценарии

UserGate NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря концепции SOAR (Security Orchestration, Automation and Response). NGFW реализует данную концепцию с помощью механизма сценариев. Сценарий является дополнительным условием в правилах межсетевого экрана, пропускной способности, контентной фильтрации, PBR, правилах защиты DoS, позволяя администратору настроить реакцию NGFW на определенные события, произошедшие за некое продолжительное время.

Примером работы сценария может быть задача по ограничению на определенное время пропускной способности для пользователя, который выбрал установленный лимит трафика.

### Настройка сценариев

Для начала работы со сценариями необходимо выполнить следующие шаги:

1. Создать сценарий.
2. Применить созданный сценарий в правилах межсетевого экрана, пропускной способности, контентной фильтрации, PBR, правилах защиты DoS.

В веб-консоли администратора сценарии создаются в разделе **Библиотеки элементов → Сценарии**.

При создании сценария необходимо указать следующие параметры:

- **Включено** — Включает или отключает сценарий.
- **Название** — Название сценария.
- **Описание** — Описание сценария.
- **Применить для** — Параметр, отвечающий за количество пользователей в правиле, к которым будет применен сценарий. Возможны варианты:
  - **Одного пользователя** — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий.
  - **Всех пользователей** — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в поле Пользователи/Группы правила.
- **Продолжительность** — длительность работы ограничивающего правила, в котором сработал сценарий.

На вкладке **Условия** задаются условия срабатывания сценария. Для каждого условия можно указать количество срабатываний за определенное время, необходимое для срабатывания сценария. Если выбрано несколько условий, то необходимо указать механизм срабатывания сценария — совпадение хотя бы одного из указанных условий, или всех условий.

## Настройка условий срабатывания сценариев

Возможны следующие условия срабатывания для использования в сценарии:

- **Категория URL** — совпадения указанных категорий UserGate URL в трафике пользователя.
- **Обнаружен вирус** — факт обнаружения вируса.
- **Приложение** — обнаружено указанное приложение в трафике пользователя.
- **СОВ** — срабатывание системы обнаружения вторжений.
- **Типы контента** — обнаружены указанные типы контента в трафике пользователя.
- **Объем трафика** — объем трафика пользователя превысил определенный лимит за указанную единицу времени.
- **Проверка состояния** — проверка состояния какого-либо ресурса, который должен быть доступен с NGFW. Проверка может осуществляться с помощью команды `ispr ping`, запроса DNS или выполнения HTTP GET.

### Категория URL

Условием срабатывания в данном случае является совпадения указанных категорий UserGate URL в трафике пользователя.

В данном условии настраиваются следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выбор категорий сайтов из библиотеки элементов или создание списка с категориями сайтов из имеющихся в библиотеке элементов.
- **Проверить URL** — возможность проверки конкретного URL на соответствие той или иной категории.

### Обнаружен вирус

Условием срабатывания в данном случае является обнаружение вируса в трафике пользователя.

Приложение

Условием срабатывания в данном случае является обнаружение определенных приложений в трафике пользователя.

В данном условии настраиваются следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выбор групп или категорий приложений из библиотеки элементов.

СОВ

Условием срабатывания в данном случае является детектирование системой COB угрозы определенного уровня.

## Типы контента

В данном условии настраиваются следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выбор типов контента из библиотеки элементов.

## Объем трафика

Условие срабатывания сценария по объему прошедшего трафика через NGFW.

|  |
|--|
|  |
|  |

В данном условии настраиваются параметры:

- **Введите размер** — предельный объем трафика, прошедшего через NGFW, при котором сработает сценарий.
- **Период** — промежуток времени за который будет посчитан объем проходящего трафика.

Т.е. если будет выбран 5 ГБ за день, то при превышении 5 ГБ трафика пользователем за 1 день, сработает данный сценарий.

## Проверка состояния

Условия срабатывания сценарии зависят от состояния сервера, запрос к которому идет с NGFW.

Возможны следующие методы проверки состояния сервера:

- Ping;
- DNS;
- HTTP GET.

Метод **Ping**.

В данном условии настраиваются следующие параметры:

- **Адрес** — IP-адрес для выполнения ICMP ping с NGFW.
- **Шлюз** — шлюз.
- **Результат** — отрицательный или положительный. Определяет, какой результат будет ожидаться от пинга сервера. Отрицательный — нет ответа по ping, положительный — ответ есть.
- **Тайм-аут подключения** — максимальное время, в течение которого клиент готов ждать ответа от сервера после успешного установления соединения.
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.

Метод **DNS**.

В данном условии настраиваются следующие параметры:

- **Адрес** — это ip адрес DNS сервера, на который посылаем DNS запросы с NGFW.
- **FQDN запроса** — доменное имя сервера, которое разрешается в рамках проверки доступности.
- **Шлюз** — шлюз.
- **Результат** — положительный или отрицательный. Определяет, какой результат будет ожидаться от запроса сервера. Отрицательный — нет ответа, положительный — ответ есть.
- **Тайм-аут подключения** — максимальное время, в течение которого клиент готов ждать ответа от сервера после успешного установления соединения.
- **Тип DNS-запроса** — тип DNS-запроса (a, aaaa, cname, ns, ptr).
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария.
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.

Тип **HTTP GET**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

В данном условии настраиваются следующие параметры:

- **Адрес** — домен для выполнения HTTP GET с NGFW.
- **Шлюз** — шлюз.
- **Результат** — положительный или отрицательный. Определяет, какой результат будет ожидаться от запроса сервера. Отрицательный — нет ответа, положительный — ответ есть.
- **Тайм-аут подключения** — максимальное время, в течение которого клиент готов ждать ответа от сервера после успешного установления соединения.
- **Тайм-аут ответа** — тайм-аут ответа для проверки выполнением HTTP GET.
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария.
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.

Пример использования сценариев

Как пример, сценарии могут использоваться в правилах межсетевого экрана для ограничения доступа в сеть, если происходит какое-либо событие, описанное в сценарии.

В данном примере реализуется следующий сценарий: для подключенных к NGFW узлов должно работать правило межсетевого экрана, блокирующее доступ в сеть на 5 минут, если на этом узле было скачано за 1 минуту 250 МБ трафика и более. В ином случае доступ в сеть через NGFW должен быть разрешен.

Создан сценарий с условием срабатывания по объему прошедшего трафика:

В межсетевом экране создано блокирующее правило, в которое добавлен созданный сценарий:

Верхнее блокирующее правило **Block by traffic** в межсетевом экране имеет более высокий приоритет по отношению к нижнему разрешающему правилу **Allow all**, но оно сработает только в случае срабатывания сценария по объему прошедшего трафика. В остальных случаях трафик будет разрешен правилом **Allow all**.

## Теги

---

Version: 7.x

Product: NGFW

Тегами называются специализированные маркеры, которые могут назначаться объектам в веб-интерфейсе для удобства их отображения, группирования и фильтрации.

**Примечание**Использование тегов доступно в версии 7.3.0 и выше.

В UserGate NGFW теги могут быть присвоены интерфейсам и всем типам правил — правилам межсетевого экрана, NAT и маршрутизации, пропускной способности, фильтрации контента, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, защиты почтового трафика, ICAP, защиты от DoS-атак, reverse-прокси, серверным и клиентским правилам VPN.

В веб-консоли администратора UserGate NGFW список всех созданных на устройстве тегов находится в **Библиотеке элементов**:

Для создания нового тега нажмите **Добавить** и заполните поля настроек тега в окне свойств:

Укажите наименование тега. Оно может иметь не более 64 символов, начинаться с символа буквы или цифры, иметь в своём составе пробел и символы: `.,()_+ - :/@.`

При необходимости для тега можно выбрать цветовую маркировку из десяти имеющихся цветов:

Опционально добавьте описание создаваемому тегу.

Помимо библиотеки элементов теги можно создавать непосредственно в свойствах маркируемых объектов — интерфейсов или правил, выбрав в поле **Теги** опцию **Добавить новый Тег**. Откроется такое же диалоговое окно создания тега, как описано выше.

Пример создания тега непосредственно в свойствах правила межсетевого экрана:

Теги могут присваиваться интерфейсам устройства. Каждому интерфейсу может быть присвоено множество тегов:

Теги могут присваиваться любым типам правил в NGFW. Пример использования тегов в правилах межсетевого экрана:

Благодаря использованию тегов объекты в веб-интерфейсе можно визуальнo группировать. Поддерживается фильтрация объектов в веб-интерфейсе по тегам как с помощью кнопки в меню инструментов, так и с помощью команд в строке поиска:

В разделах настроек правил или интерфейсов есть инструмент для групповой работы с тегам. При выделении сразу нескольких объектов становится активной кнопка **Управление тегами** в панели инструментов:

С помощью инструмента управления тегами можно добить и удалить теги множеству объектов одновременно:

Результат одновременного массового добавления и удаления тегов в правила межсетевого экрана:

Работа с тегами также поддерживается в интерфейсе командной строки. Подробнее о работе с тегами в CLI читайте в статье [Настройка библиотек](#).

