Table of Contents

Table of Contents 1
Библиотеки элементов 2
- Общие сведения 3
- Морфология 4
- IP-адреса 6
- User agent браузеров 8
- Типы контента 9
- Списки URL 10
- Календари 13
- Полосы пропускания 14
- Шаблоны страниц 15
- Категории URL 17
- Измененные категории URL 23
- Почтовые адреса 24
- Номера телефонов 25
- Профили оповещений 26
- Профили LLDP 27
- Профили SSL 28
- Профили пересылки SSL 30
- Профили BFD 31
- Syslog-фильтры UserID агента 33
- Сценарии 34
- Теги 36

Библиотеки элементов

Общие сведения

Version: 7.5.x

Product: SWG

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

Первоначальные данные библиотек поставляются вместе с продуктом. Вы можете добавлять необходимые 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 SWG».

Морфология

Product: SWG
Version: 7.5.x

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, UserGate SWG 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 UserGate SWG использует встроенные словари русского, английского, японского, арабского и немецкого языков.

Существует возможность подписки на словари, предоставляемые компанией UserGate. Эти словари нельзя редактировать. Для использования этих словарей необходима соответствующая лицензия. Подробнее о лицензии на продукт — в разделе «Лицензирование».

Наименование словаря	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 создания собственного морфологического списка:

1. В разделе **Настройки → Библиотеки → Морфология** в блоке **Списки** морфологии нажмите **Добавить**, укажите название нового списка и его вес.

2. В блоке **Слова** нажмите **Добавить**, укажите слова или фразы с соответствующими им весами. При добавлении слов 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.

Вы можете создавать свои словари и централизованно распространять их на все устройства UserGate, имеющиеся в организации. Для создания такой базы:

1. Создайте файл с необходимыми фразами. Например, файл list.txt может содержать список слов в следующем формате:

```
!word1
!word2
!word3
word4 50
...
Lastword
```

Вес слова можно указать. По умолчанию он равен 100.

2. Создайте архив, содержащий этот файл. Например, ZIP-архив с именем list.zip.

3. Создайте файл с версией словаря. Например, файл version.txt, внутри него указан номер версии базы. Необходимо инкрементировать это значение при каждом обновлении морфологического словаря.

4. Разместите файлы (list.zip и version.txt) на веб-сервере.

5. Создайте морфологический список и укажите URL для обновления словаря.

На каждом устройстве UserGate создайте морфологическую базу. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. Устройство UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений.

Вы можете выбрать одно из предустановленных значений расписания 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 проверка обновлений должна выполняться каждый час.

Дефис (-) — для указания диапазона значений.

Запятая (,) — в качестве разделителя значений.

Косая черта (/) — для указания шага между значениями.

ПримечаниеПри 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. Это сократит количество возможных вариантов фраз, но оставит все фразы с требуемым смыслом.

Устройство 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
```

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

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Для фильтрации по морфологическому содержанию страницы создайте правило фильтрации контента, содержащее один или несколько морфологических списков.Подробнее — в разделе «Фильтрация контента».

IP-адреса

Product: SWG
Version: 7.5.x

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил ГUserGate SWG. Первоначальный список адресов поставляется вместе с продуктом. Вы можете добавлять необходимые элементы в процессе работы. Для добавления нового списка адресов выполните следующие шаги:

Шаг	Описание
1. Создайте список.	На панели **Группы** нажмите **Добавить**: • Укажите название списка IP-адресов. • Добавьте описание списка (опционально). • Укажите уровень угрозы адресов в списке (параметр для визуального отображения, какие адреса не представляют особой угрозы, а какие лучше запретить). • Выберите тип списка (локальный или обновляемый по URL обновления)
2. Укажите адрес обновления списка (для обновляемых списков).	Укажите адрес сервера, где находится обновляемый список
3. Добавьте IP-адреса.	На панели **Адреса из выбранной группы** нажмите **Добавить** и укажите адреса. 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

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

Шаг	Описание
1. Создайте файл с необходимыми IP-адресами.	Создайте файл list.txt со списком адресов. Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: x.x.x.x y.y.y.y z.z.z.z
2. Создайте архив, содержащий этот файл.	Поместите файл в архив zip с именем list.zip
3. Создайте файл с версией списка.	Создайте файл version.txt, внутри него укажите номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
4. Разместите файлы на веб-сервере.	Разместите у себя на сайте list.zip и version.txt, чтобы они были доступны для скачивания
5. Создайте список IP-адресов и укажите URL для обновления.	На каждом UserGate SWG создайте список IP-адресов. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. **Примечание**URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Вы можете выбрать одно из предустановленных значений расписания 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 проверка обновлений должна выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями.

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate SWG 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

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

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

User agent браузеров

Product: SWG
Version: 7.5.x

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

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

Шаг	Описание
1. Создайте список Useragent.	В панели **Категории** нажмите **Добавить** и укажите название нового списка User agent
2. Добавьте необходимые User agent браузеров в новый список.	В панели **Шаблоны user agent** добавьте необходимый User agent. Список строк User agent можно найти по ссылке
3. Создайте правило фильтрации контента, содержащее один или несколько списков.	Подробнее — в разделе «Фильтрация контента»

Вы можете создавать свои списки User agent и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Шаг	Описание
1. Создайте файл с необходимыми User agent.	Создайте файл list.txt со списком Useragent.
2. Создайте архив, содержащий этот файл.	Поместите файл в архив zip с именем list.zip
3. Создайте файл с версией списка.	Создайте файл version.txt, внутри него укажите номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
4. Разместите файлы на веб-сервере.	Разместите у себя на сайте list.zip и version.txt, чтобы они были доступны для скачивания.
5. Создайте список User agent и указать URL для обновления.	На каждом UserGate SWG создайте список User agent. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UseGate SWG будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Вы можете выбрать одно из предустановленных значений расписания 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 проверка обновлений должна выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями.

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate SWG 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-сумма list.zip, после чего сохраняется в формате md5. Например, содержимое файла list.zip.md5:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Типы контента

Product: SWG
Version: 7.5.x

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. Такие списки типов контента нельзя редактировать, их можно использовать при определении правил фильтрации контента. Для использования этих списков необходима соответствующая лицензия. Подробнее о лицензии на продукт — в разделе «Лицензирование».

Для фильтрации по типу контента выполните следующие действия:

Шаг	Описание
1. Создайте список типов контента. Если используется предопределенный список UserGate, перейдите к шагу 3	В панели **Категории** нажмите **Добавить**, укажите название нового списка типа контента; опционально — описание списка и URL обновления
2. Добавьте необходимые типы контента в новый список	Добавьте необходимый тип контента в список в формате MIME. Различные типы контента и их описание доступны по ссылке. Например, для блокировки документов типа *.doc необходимо добавить тип контента «application/msword»
3. Создайте правило фильтрации контента, содержащее один или несколько списков	Подробнее — в разделе «Фильтрация контента»

Вы можете создавать свои списки типов контента и централизованно распространять их на все узлы UserGate. Для создания такого списка необходимо выполнить следующие действия:

Шаг	Описание
1. Создайте файл с необходимыми типами контента	Создать файл list.txt со списком типов контента
2. Создайте архив, содержащий этот файл	Поместить файл в архив zip с именем list.zip
3. Создайте файл с версией списка	Создать файл version.txt, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
4. Разместите файлы на веб-сервере	Разместить у себя на сайте list.zip и version.txt, чтобы они были доступны для скачивания
5. Создайте список типа контента и укажите URL для обновления	На каждом UserGate SWG создайте список типа контента. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Вы можете выбрать одно из предустановленных значений расписания 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 проверка обновлений должна выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate SWG 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

Ее 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: SWG
Version: 7.5.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 SWG — 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 по ссылке
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Список доступен по ссылке

Вы также можете создать собственные списки URL в веб-консоли или в интерфейсе командной строки UserGate SWG.

Для создания списка в веб-консоли:

1. В разделе **Настройки → Библиотеки → Списки URL** нажмите **Добавить** и задайте название и описание нового списка.

2. Выберите тип списка (локальный или обновляемый). Для обновляемого списка укажите URL обновления и настройте расписание скачивания обновлений.

3. 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.
   ПримечаниеПри 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.

4. Добавьте необходимые записи в новый список.

   В списках можно использовать специальные символы:

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

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 или *yahoo.com*	Блокируется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com; mail.yahoo.com; а также: qweryahoo.com	Блокируется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyahoo.com/	Блокируются любые вхождения yahoo.com: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyahoo.com/ Не блокируются вхождения типа: https://ya.ru/YAHoo.cOM	Блокируются любые вхождения yahoo.com: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyahoo.com/ https://ya.ru/YAHoo.cOM
^mail.yahoo.com$	Заблокирован только mail.yahoo.com	Заблокированы: http://mail.yahoo.com; https://mail.yahoo.com; а также любые ссылки на этом домене, например: http://mail.yahoo.com/personal-finance 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: http://mail.yahoo.com; https://mail.yahoo.com; и любые ссылки на этом домене, например: https://mail.yahoo.com/personal-finance т. к. при преобразовании списка остается только домен, слеш в этом случае удалится и реально в списке будет: ^mail.yahoo.com$ 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: http://finance.yahoo.com; https//finance.yahoo.com; и любые ссылки на этом домене, например: http://finance.yahoo.com/personal-finance/ т.к. после преобразования в списке останется только: ^finance.yahoo.com$ Т. е. блокируется весь домен finance.yahoo.com и все URL этого домена	Заблокируется только запрос https://finance.yahoo.com/personal-finance/ Не заблокируется: http://finance.yahoo.com/personal-finance/ и любое изменение регистра букв в URL: https://finance.yahoo.com/personal-financE/	Заблокируется только запрос https://finance.yahoo.com/personal-finance/ и любое изменение регистра букв в URL: https://finance.yahoo.com/Personal-financE/. Не заблокируется: 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: http://yahoo.com/12345/whatever/; https://yahoo.com/12345/whatever/; т.к. после преобразования в списке будет: ^yahoo.com 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 SWG. 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 SWG создайте список URL. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

ПримечаниеURL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/.

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 SWG 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: 7.5.x
Product: SWG

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

1. Создайте календарь.В разделе **Настройки → Библиотеки → Календари** на панели **Группы** нажмите **Добавить**, укажите название календаря и его описание.

2. Добавить временные интервалы в календарь На панели **Элементы** нажмите **Добавить** и добавьте интервал. Задайте название интервалу и укажите временные параметры.

Полосы пропускания

Product: SWG
Version: 7.5.x

Элемент библиотеки **Полоса пропускания** определяет скорость передачи данных, которую вы можете в дальнейшем использовать в правилах управления полосой пропускания. Подробнее о правилах управления полосой пропускания — в разделе «Пропускная способность».

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

1. Создайте полосу пропускания. В разделе **Настройки → Библиотеки → Полосы** пропускания нажмите **Добавить**, задайте название и описание полосы пропускания.

2. Укажите скорость полы пропускания в Кбит/сек.

3. Укажите значение DSCP для QoS. Это опциональный параметр. Если установлен, будет прописываться в каждый IP-пакет. Диапазон от 0 до 63.

Шаблоны страниц

Product: SWG
Version: 7.5.x

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

Шаблон	Описание
Blockpage (EN) и **Blockpage (RU)**	Стандартные шаблоны блокировки на английском и русском языках. Подробнее о настройке этих шаблонов — в разделе ниже
Captive portal user auth (EN) и **Captive portal user auth (RU)**	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
Captive portal user auth + policy (EN) и **Captive portal user auth + policy (RU)**	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
Captive portal: email auth (EN) и **Captive portal: email auth (RU)**	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 **Оповещения** в Captive-профиле
Captive portal: SMS auth (EN) и **Captive portal: SMS auth (RU)**	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 **Оповещения** в Captive-профиле
Captive portal policy (EN) и **Captive portal policy (RU)**	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 **Принять политику** в качестве метода аутентификации в Captive-профиле
Captive portal user session (EN) и **Captive portal user session (RU)**	Шаблоны на английском и русском языках, с помощью которых пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps
Content warning (EN) и **Content warning (RU)**	Шаблоны на английском и русском языках, содержащие страницу предупреждения, отображаемую при срабатывании правила контентной фильтрации с действием **Предупредить**
FTP client (EN) и **FTP client (RU)**	Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP
SSL VPN (EN) и **(RU)**	Шаблоны на английском и русском языках для отображения страницы веб-портала
SSL VPN RDP (EN) и **(RU)**	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал
SSL VPN SSH (EN) и **(RU)**	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал
TOTP INIT PAGE (EN) и **TOTP INIT PAGE (RU)**	Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей
NETWRK ERROR PAGE (RU) и **NETWORK ERROR PAGE (EN)**	Шаблоны на русском и английском языках для отображения страницы сетевых ошибок от прокси-сервера

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.
- Имя узла UserGate SWG, заблокировавшего запрос.
- Названия групп, в которых состоит пользователь.
- 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.

ПримечаниеНе 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.

ПримечаниеНе 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

Product: SWG
Version: 7.5.x

Элемент библиотеки **Категории URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. Например, вы можете создать группу категорий «Бизнес категории» и поместить в нее необходимые категории.

Для использования категорий UserGate URL filtering требуется наличие специальной лицензии.

Первоначальный список поставляется вместе с продуктом. Вы можете добавлять необходимые элементы в процессе работы.

Наименование	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 срабатывани
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:

1. Создайте группу категорий. В разделе **Настройки → Библиотеки → Категории URL** на панели **Группы URL категорий** нажмите **Добавить** и укажите название группы.

2. Добавьте категории. Выделите созданную группу и на панели **Категории** нажмите **Добавить**. 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 обхождения 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 читах
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

ID	Уровень риска	Название	Описание
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
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 развлечениям 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

ID	Уровень риска	Название	Описание
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
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, аборты, 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

ID	Уровень риска	Название	Описание
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
84	Низкий (2)	Обновления / Updates	Сайты обновлений программного обеспечения, обновлений операционных систем, обновлений
85	Средний (3)	Чат-боты искусственного интеллекта / Chat-bot AI	Сайты, предоставляющие доступ к чат-ботам искусственного интеллекта, подобным Chat GPT
97	Низкий (2)	Репутация: Низкий риск / 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 риск / Reputation: 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 риск / Reputation: High risk	Сайты с высоким репутационным риском. Сайты с известными уязвимостями

Измененные категории URL

Product: SWG
Version: 7.5.x

Элемент библиотеки **Измененные категория URL** позволяет администратору назначить определенным сайтам категории, отличные от категорий, назначенных техническими специалистами UserGate. Такая потребность может возникнуть в случае некорректного категорирования сайтов или в случае, если требуемый сайт не имеет назначенной ему категории. Для переопределения категории сайта выполните следующие действия:

1. Проверьте первоначальную категорию сайта. В разделе **Настройки → Библиотеки → Измененные категории URL** введите требуемый адрес сайта в строку проверки и нажмите **Проверить категорию**.

2. Назначьте новую категорию. Если полученная категория не совпадает с требуемой, нажмите **Добавить** и назначьте до двух новых категорий.

После успешного изменения категории сайт будет отображаться в списке сайтов с измененными категориями. Для него также будет указаны дата изменения категории, администратор, выполнивший данное изменение, его оригинальные и новые категории.

При последующей проверке категорий для данного сайта в качестве категорий будут возвращены только новые категории и специальная категория, в которую включаются все сайты с измененными категориями — **Переопределенные пользователем категории**.

Вы можете экспортировать списки сайтов с измененными категориями или импортировать любые списки сайтов и назначить им требуемые категории.

Почтовые адреса

Version: 7.5.x
Product: SWG

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:

1. Создайте группу почтовых адресов. В разделе **Настройки → Библиотеки → Почтовые адреса** на панели **Группы почтовых адресов** нажмите **Добавить** и укажите название группы.

2. Добавьте почтовые адреса в группу. Выделите созданную группу, на панели **Почтовые адреса** нажмите **Добавить** и добавьте необходимые почтовые адреса.

Вы можете создавать собственные обновляемые списки почтовых адресов и централизованно распространять их на все узлы UserGate. Для создания таких списков выполните следующие действия:

1. Создайте текстовый файл (например, list.txt) со списком адресов.

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 SWG создайте список адресов. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

ПримечаниеURL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/.

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 SWG 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

Номера телефонов

Product: SWG
Version: 7.5.x

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров:

1. Создайте группу телефонных номеров. В разделе **Настройки → Библиотеки → Номера телефонов** на панели **Группы телефонных номеров** нажмите **Добавить** и укажите название группы.

2. Добавьте номера телефонов в группу. Выделите созданную группу, в панели **Группа телефонных номеров** нажмите **Добавить** и добавьте необходимые номера.

Вы можете создавать собственные обновляемые списки и централизованно распространять их на все узлы UserGate. Для создания таких списков выполните следующие действия:

1. Создайте текстовый файл (например, list.txt) со списком номеров телефонов.

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 SWG создайте список URL. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

ПримечаниеURL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/.

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 SWG 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
```

Профили оповещений

Product: SWG
Version: 7.5.x

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается два 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 в разделе **Настройки → Библиотеки → Профили оповещений** нажмите **Добавить**, выберите **Добавить профиль оповещения SMTP** и укажите необходимые параметры профиля.

Параметр	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-сервер
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP в разделе **Настройки → Библиотеки → Профили оповещений** нажмите **Добавить**, выберите **Добавить профиль оповещения SMPP** и укажите необходимые параметры профиля.

Параметр	Описание
Название	Название профиля
Описание	Описание профиля
Хост	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS сообщени
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 LLDP

Product: SWG
Version: 7.5.x

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 на сетевом устройстве.

Для создания профиля безопасности в разделе **Настройки → Библиотеки → Профили LLDP** нажмите **Добавить** и укажите необходимые параметры профиля.

Параметр	Описание
Название	Название профиля LLDP
Описание	Описание профиля LLDP
Статус порта	Режим: • **Приём и передача данных LLDP** — UserGate SWG будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей. • **Только приём данных LLDP** — UserGate SWG не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • **Только передача данных LLDP** — UserGate SWG будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей

Профили SSL

Product: SWG
Version: 7.5.x

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 в разделе **Настройки → Библиотеки → Профили SSL** нажмите **Добавить** и укажите необходимые параметры профиля.

Параметр	Описание
Название	Название профиля SSL
Описание	Описание профиля SSL
Протоколы SSL	**Минимальная версия TLS** — устанавливает минимальную версию TLS, которая может быть использована в данном профиле. **Максимальная версия TLS** — устанавливает максимальную версию TLS, которая может быть использована в данном профиле. Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем
Наборы алгоритмов шифрования	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: • TLS AES 128 CCM SHA256 • TLS AES 128 GCM SHA256 • TLS AES 256 GCM SHA384 • TLS DHE DSS WITH 3DES EDE CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA256 • TLS DHE DSS WITH AES 128 GCM SHA256 • TLS DHE DSS WITH AES 256 CBC SHA • TLS DHE DSS WITH AES 256 CBC SHA256 • TLS DHE DSS WITH AES 256 GCM SHA384 • TLS DHE RSA WITH 3DES EDE CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA256 • TLS DHE RSA WITH AES 128 GCM SHA256 • TLS DHE RSA WITH AES 256 CBC SHA • TLS DHE RSA WITH AES 256 CBC SHA256 • TLS DHE RSA WITH AES 256 GCM SHA384 • TLS ECDH ECDSA WITH 3DES EDE CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA256 • TLS ECDH ECDSA WITH AES 128 GCM SHA256 • TLS ECDH ECDSA WITH AES 256 CBC SHA • TLS ECDH ECDSA WITH AES 256 CBC SHA384 • TLS ECDH ECDSA WITH AES 256 GCM SHA384 • TLS ECDH RSA WITH 3DES EDE CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA256 • TLS ECDH RSA WITH AES 128 GCM SHA256 • TLS ECDH RSA WITH AES 256 CBC SHA • TLS ECDH RSA WITH AES 256 CBC SHA384 • TLS ECDH RSA WITH AES 256 GCM SHA384 • TLS ECDHE ECDSA WITH 3DES EDE CBC SHA

Параметр	Описание
	• TLS ECDHE ECDSA WITH AES 128 CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA256
	• TLS ECDHE ECDSA WITH AES 128 GCM SHA256 • TLS ECDHE ECDSA WITH AES 256 CBC SHA • TLS ECDHE ECDSA WITH AES 256 CBC SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH 3DES EDE CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA256 • TLS ECDHE RSA WITH AES 128 GCM SHA256 • TLS ECDHE RSA WITH AES 256 CBC SHA • TLS ECDHE RSA WITH AES 256 CBC SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384 • TLS RSA WITH 3DES EDE CBC SHA • TLS RSA WITH AES 128 CBC SHA • TLS RSA WITH AES 128 CBC SHA256 • TLS RSA WITH AES 128 GCM SHA256 • TLS RSA WITH AES 256 CBC SHA • TLS RSA WITH AES 256 CBC SHA256 • TLS RSA WITH AES 256 GCM SHA384
Установка алгоритмов шифрования для стандартных протоколов	Этот раздел можно использовать для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS. Администратор может указать в поле **Выберите протокол для установки алгоритмов** необходимые версии протоколов TLS, нажать на кнопку **Применить**, и алгоритмы, соответствующие выбранной версии протокола автоматически будут отмечены. Можно последовательно добавить несколько версий протокола TLS

По умолчанию в продукте создано несколько профилей SSL, которые могут быть использованы администратором, изменены или удалены при необходимости.

Профиль	Описание
Default SSL profile	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: • Правилах инспектирования трафика SSL. • Для страницы авторизации Captive-портала. • Для страницы блокировки. • В веб-портале
Default SSL profile (TLSv1.3)	Содержит алгоритмы и подписи, соответствующие версии TLS v.1.3. По умолчанию не используется
Default SSL profile (web console)	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 **Важно!** Изменение этого профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа к веб-консоли.

Профили пересылки SSL

Product: SWG
Version: 7.5.x

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 в разделе **Настройки → Библиотеки → Профили пересылки SSL** нажмите **Добавить** и укажите необходимые параметры профиля.

Параметр	Описание
Название	Название профиля пересылки SSL
Описание	Описание профиля пересылки SS
Тип пересылки	Доступные типы пересылки: • **L2** — при настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. • **L3-туннель** — копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адреса источника и назначения
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

Профили BFD

Product: SWG
Version: 7.5.x

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 **Настройки → Библиотеки → Профили BFD** нажать **Добавить** и указать необходимые параметры профиля.

Параметр	Описание
Название	Название профиля BFD
Описание	Опциональное описание профиля
Определить множитель	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. Например, если интервал передачи равен 300 мс, а множитель — 3, то локальная система будет обнаруживать сбои только через 900 мс отсутствия приёма пакетов
Интервал приёма	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. Значение по умолчанию — 50 мс
Интервал передачи	Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами. Значение по умолчанию — 50 мс
Время получения echo	Минимальный интервал, через который система способна принимать echo-пакеты. Значение по умолчанию — 50 мс
Время отправки echo	Минимальный интервал передачи, через который система будет способна отправлять echo-пакеты BFD. Значение по умолчанию — 50 мс
Echo режим	Включение/отключение режима передачи Echo. По умолчанию этот режим отключён. 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. 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 SWG, 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

Параметр	Описание
Пассивный режим	Включение/отключение пассивного режима. При работе в пассивном режиме система ждёт управляющие пакеты от соседей и отвечает на них в случае их получения. Эта функция полезна, когда маршрутизатор выступает в роли центрального узла звездообразной сети, и требуется избежать отправки ненужных управляющих пакетов BFD. По умолчанию используется активный режим. При работе в активном режиме узел отправляет управляющие пакеты соседнему узлу. Оба узла не могут работать в пассивном режиме; хотя бы один из них (или оба) должны работать в активном режиме
Минимальное время жизни	Только для сеансов с несколькими переходами. 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. Установка данного значения необходима для ужесточения требований к проверке пакетов во избежание получения управляющих пакетов BFD от других сессий. Значение по умолчанию равно 254 (это означает, что ожидается только один переход между этой системой и аналогом)

Syslog-фильтры UserID агента

Product: SWG

Version: 7.5.x

Technology: Identification and Authentication

При использовании syslog в качестве источников событий UserGate SWG производит фильтрацию событий в соответствии с указанными syslog-фильтрами UserID агента. Фильтры syslog представляют из себя стандартные Regexp-выражения, которые пользователь может писать и сам. В стандартной поставке представлены три вида фильтров:

Наименование	Описание
SSH Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей по протоколу SSH в журналах syslog
Unix PAM Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей посредством технологии **Pluggable Authentication Modules** (PAM) в журналах syslog
UserGate WEC Agent	Фильтр, предназначенный для отслеживания событий, переданных через syslog из UserID агента для AD/WEC-серверов

ПримечаниеИспользуя правила Regexp, возможно написание дополнительных правил. Таким образом, фильтры syslog представляют из себя универсальный инструмент, который можно использовать практически в любых случаях.

Найденные события отображаются на вкладке **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

Product: SWG
Version: 7.5.x

Сценарии является дополнительным условием в правилах контентной фильтрации, позволяющим администратору настроить реакцию UserGate SWG на определенные события, произошедшие за некоторое время.

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

Настройка сценариев

Для работы со сценариями необходимо:

1. Создать сценарий.
2. Применить созданный сценарий в правилах контентной фильтрации.

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

Для создания сценария нажмите **Добавить** и укажите следующие параметры:

- На вкладке **Общие**:
  - **Включено** — включение или отключение сценария.
  - **Название** — название сценария.
  - **Описание** — описание сценария.
  - **Применить для** — параметр, отвечающий за количество пользователей в правиле, к которым будет применен сценарий:
    - **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** задайте условия срабатывания сценария. Для каждого условия можно указать количество срабатываний за определенное время, необходимое для срабатывания сценария. Если выбрано несколько условий, укажите 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.
- **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 UserGate SWG. Проверка может осуществляться с помощью команды icmp ping, запроса DNS или выполнения HTTP GET.

Категория URL

Условием срабатывания в этом случае является совпадение указанных категорий UserGate URL в трафике пользователя.

Для настройки этого условия укажите следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выберите категории сайтов из библиотеки или создайте список с категориями сайтов из имеющихся в библиотеке элементов.

Вы можете проверить конкретный URL на соответствие той или иной категории, для этого укажите URL в строке проверки и нажмите **Проверить URL**.

Обнаружен вирус

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

Типы контента

Для настройки этого условия укажите следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выберите типы контента из библиотеки элементов или создайте собственный тип контента.

Объем трафика

Условие срабатывания сценария по объему прошедшего трафика через UserGate SWG.

Для настройки этого условия укажите следующие параметры:

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

Например, если будет выбран объем трафика 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 от UserGate SWG.

Возможны следующие методы проверки состояния сервера:

- Ping;
- DNS;
- HTTP GET.

Метод **Ping**.

Для настройки этого метода укажите следующие параметры:

- **Адрес** — IP-адрес для выполнения ICMP ping с UserGate SWG.
- **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** — интервал времени, в течение которого клиент будет ждать ответ от сервера после успешного установления соединения.
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария.
- **За интервал** — интервал, в течение которого будут учитываться срабатывания.

Метод **DNS**.

Для настройки этого метода укажите следующие параметры:

- **Адрес** — IP-адрес DNS-сервера, на который посылаются DNS-запросы с UserGate SWG.
- **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** — интервал времени, в течение которого клиент будет ждать ответ 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 будут учитываться срабатывания.

Метод **HTTP GET**.

Для настройки этого метода укажите следующие параметры:

- **Адрес** — домен для выполнения HTTP GET с UserGate SWG.
- **Шлюз** — шлюз.
- **Результат** — положительный или отрицательный. Определяет, какой результат будет ожидаться от запроса сервера. Отрицательный — нет ответа, положительный — ответ есть.
- **Тайм-аут подключения** — интервал времени, в течение которого клиент будет 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 будут учитываться срабатывания.

Теги

Product: SWG
Version: 7.5.x

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

В UserGate SWG теги могут быть присвоены интерфейсам и всем типам правил — правилам межсетевого экрана, NAT и маршрутизации, пропускной способности, фильтрации контента, веб-безопасности, инспектирования SSL, ICAP, reverse-прокси.

В веб-консоли администратора UserGate SWG список всех созданных на устройстве тегов находится в разделе **Настройки → Библиотеки → Теги**:

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.

Благодаря использованию тегов объекты в веб-интерфейсе можно визуально 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 тегами. 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.

Работа с тегами также поддерживается в интерфейсе командной строки. Подробнее о работе с тегами в CLI — в разделе « Настройка библиотек».