Table of Contents

Table of Contents 1
Журналы и отчеты 2
- Журналы 3
  - Описание 4
  - Журнал событий 5
  - Журнал веб-доступа 6
  - Журнал СОВ 7
  - Журнал АСУ ТП 8
  - Журнал инспектирования SSH 9
  - История поиска 10
  - Поиск и фильтрация данных 11
  - Экспорт журналов 13
  - Журнал трафика 16
- Отчеты 17
  - Описание 18
  - Шаблоны отчетов 19
  - Правила отчетов 20
  - Созданные отчеты 22

Журналы и отчеты

Журналы

Описание

Version: 5.x, 6.1.9, 7.0.1
Documentation: ☑

UserGate журналирует все события, которые происходят во время его работы, и записывает их в следующие журналы:

- **Журнал событий** — события, связанные с изменением настроек NGFW, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных NGFW.
- **Журнал трафика** — подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing. Для регистрации данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing.
- **Журнал СОВ** — события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал АСУ ТП** — события, регистрируемые правилами контроля систем АСУ ТП.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** — поисковые запросы пользователей в популярных поисковых системах.

Управление журналами автоматизировано: журналы циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство.

ПримечаниеЗаписи журнала событий никогда не ротируются.

Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных будут отображены в журнале событий. В случае, если подключен LogAn, то запись будет отображена в журнале событий Log Analyzer.

Журнал событий

Documentation:
Version: 5.x, 6.1.9, 7.0.1
Product: NGFW

Журнал событий отображает события, связанные с изменением настроек NGFW, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал или VPN, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал веб-доступа

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL, Веб-безопасности, Captive-портала в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Категории сайтов.
- Приложение.
- Протокол прикладного уровня.
- HTTP метод.
- Код ответа HTTP.
- Тип контента (если присутствует).
- Информация.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Операционная система.
- User-agent браузер.

ПримечаниеВ столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик после срабатывания всех правил на этом запросе.
Если правила требуют анализа ответа от веб-сервера, то трафик ответа также будет подсчитан и учтён одинаковый, в том числе у первого сработавшего на этом запросе правила (bypass captive, decrypt). Таким образом, учитывается весь прошедший трафик и указывается одно и то же значение каждому правилу, сработавшему на этом запросе.
Если анализ ответа от веб-сервера для правил не требуется, то весь остальной трафик не учитывается.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал СОВ

Version: 6.1.9
Product: UserGate NGFW
Documentation:

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры СОВ, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Файлы Pcap.
- Узел UserGate, на котором произошло событие.
- Время.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Сигнатуры.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал АСУ ТП

Version: 6.1.9, 7.0.1
Product: NGFW, LogAn
Documentation: ☑

Журнал АСУ ТП отображает срабатывания правил автоматизированной системы управления технологическим процессом, для которых включена функция журналирования. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время.
- Действие.
- Правило.
- Зона источника.
- IP-адрес источника.
- IP-адрес назначения.
- Порт назначения.
- Протокол АСУ ТП.
- Команда АСУ ТП.
- Адрес регистра.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал инспектирования SSH

Version: 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH, для которых включено журналирование. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время.
- Пользователь.
- Действие.
- Правило.
- Команда.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

История поиска

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation:

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Поиск и фильтрация данных

Version: 6.1.9
Product: UserGate NGFW
Documentation:

Количество записей, регистрируемых в журналах, как правило, очень велико, и не все поля доступны в базовом режиме просмотра. UserGate предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнения всех условий, заданных в запросе.
OR или or	Логическое ИЛИ, достаточно выполнения одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, ip!=172.16.31 будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date<='2019-03-28T20:59:59' AND statusCode=303
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date>="2019-03-13T21:00:00" AND statusCode=200
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date < '2019-03-28T20:59:59' AND statusCode=404
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, (statusCode>200 AND statusCode<300) OR (statusCode=404)
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')

Наименование	Описание
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, несодержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, browser ~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, browser !~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные.

При составлении расширенного запроса UserGate показывает возможные варианты названия полей, применимых к ним операторов и возможных значений, облегчая оператору системы формирование сложных запросов. Список полей и их возможных значений может отличаться для каждого из журналов.

При переключении режима поиска с основного на расширенный UserGate автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

Экспорт журналов

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation:

Функция экспортирования журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал СОВ.
- Журнал трафика.
- Журнал АСУ ТП. (в версиях 6+)
- Журнал инспектирования SSH. (в версиях 6+)

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

ПримечаниеЕсли в настройках указан Log Analyzer, то обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером LogAn.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Опциональное поле для описания правила.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. • Журнал веб-доступа. • Журнал СОВ. • Журнал трафика. • Журнал АСУ ТП. • Журнал инспектирования SSH. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в Приложение 3. Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog — TCP или UDP.

Наименование	Описание
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog -- RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Тревога**: состояние, требующее незамедлительного вмешательства. • **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • **Ошибки**: в системе возникли ошибки. • **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками. • **Информативная**: информационные сообщения.
Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Сообщения пользовательские**. • **Системный сервис**. • **Безопасность/авторизация**. • **Аудит**. • **Тревога**. • **Local 0**. • **Local 1**. • **Local 2**. • **Local 3**. • **Local 4**. • **Local 5**. • **Local 6**. • **Local 7**.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.

Наименование	Описание
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. 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: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • 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.
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки. Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день.

Журнал трафика

Version: 6.1.9
Product: NGFW
Documentation:

Журнал трафика отображает события срабатывания правил межсетевого экрана и правил NAT, в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- NAT IP-адрес источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP-адрес назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов отправлено/получено.

ПримечаниеВ столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик, учтенный в момент срабатывания журналирующего правила.
Если в настройках журналирования в правиле выбрано: "Журналировать каждый пакет", то значения учтенного трафика в журнале будут кумулятивно нарастать в течение сессии.
Если в настройках журналирования в правиле выбрано: "Журналировать начало сессии", будет учтен всего один или несколько пакетов, необходимых для срабатывания этого правила.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Отчеты

Описание

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел **Отчеты** состоит из трех подразделов — **Шаблоны**, **Правила отчётов** и **Созданные отчеты**. Чтобы создать отчет необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета.	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет.	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
Шаг 3. Получить отчет.	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе **Созданные отчеты.**

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.
ПримечаниеВ отчетах по трафику (кроме отчетов веб-доступа) используются данные из компонента Netflow. Отчеты веб-доступа по трафику используют данные из журналов (домены, URL-категории и т.п.).

Шаблоны отчетов

Documentation:
Version: 5.x, 6.1.9, 7.0.1

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией-разработчиком UserGate.

Список шаблонов отчетов, сгруппированных по категориям:

- **Captive-портал** — группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **СОВ** — группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **Сетевая активность** — группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** — группа шаблонов авторизации через SSL VPN.
- **Трафик** — группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- **VPN** -- группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** — группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

Правила отчетов

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Включено	Включение/отключения отчета.
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчета	Выбор языка, который будет использован в отчете.
Диапазон	Диапазон времени, за который необходимо подготовить отчет.
Формат отчета	Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет. **Важно!** Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Для шаблонов **Подробный список всех посещенных URL** и **Подробный список всех посещенных сайтов** автоматически используется формат CSV, независимо от выбранного формата.
Количество записей	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
Количество в группировке (если применимо)	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
Пользователи	Задает пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.
Расписание	Выбор расписания для создания отчетов. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. 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: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7 • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23" 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.

Наименование	Описание
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: • Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. • От — имя отправителя письма. • Тема письма — тема письма (subject). • Тело письма — содержимое письма. • Получатели — список получателей письма. Получатели должны быть добавлены в списки библиотеки **Почтовые адреса**.

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

ПримечаниеДля того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать на кнопку Запустить сейчас. Готовый отчет после создания будет доступен в разделе Созданные отчеты.

Созданные отчеты

Documentation:
Version: 6.1.9, 5.x

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией разработчиком UserGate.

Список шаблонов отчетов, сгруппированных по категориям:

- **Captive-портал** - группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **События** - группа шаблонов по событиям, регистрируемым в журнале событий.
- **СОВ** - группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **Сетевая активность** - группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** - группа шаблонов авторизации через SSL VPN.
- **Трафик** - группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- **VPN** -- группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** - группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).