Table of Contents

Table of Contents 1
Диагностика и мониторинг 2
Средства диагностики и мониторинга 3
Мониторинг состояния устройства по протоколу SNMP 6

Documentation: ☑
Product: SWG
Version: 7.5.x

Вкладка веб-интерфейса **Диагностика и мониторинг** содержит набор инструментов для контроля состояния системы, проверки сетевой связности и обнаружения неисправностей.

Мониторинг

В разделе **Диагностика и мониторинг → Мониторинг** вы можете получить информацию о текущем состоянии сетевых соединений и маршрутизации на устройстве. Здесь отображаются:

- данные о пользовательских сессиях;
- активных соединениях с веб-порталом;
- маршрутизации.

Мониторинг трафика

В разделе **Диагностика и мониторинг → Мониторинг → Мониторинг трафика** выводится список всех пользовательских соединений, установленных через UserGate SWG в реальном времени.

Каждое соединение характеризуется уникальным сочетанием адреса источника, адреса назначения и имени пользователя (если пользователь определен). Отображаются мгновенные значения скорости передачи (TX) и скорости приема (RX) данных через соединение.

Имеется возможность сортировки выводимых данных по каждому столбцу.

ПримечаниеПроцесс вывода списка соединений со всеми атрибутами требует большего количества вычислительных ресурсов устройства и при большом объеме передаваемого трафика может приводить к высокой загрузке процессора. Не рекомендуется держать данную страницу открытой во избежание излишней нагрузки на устройство.

Непосредственно на странице мониторинга трафика вы можете:

- заблокировать соединение, создав блокирующее правило межсетевого экрана;
- ограничить пропускную способность, создав правило ограничения пропускной способности для выбранного из списка IP-адреса источника.

Чтобы создать блокирующее правило межсетевого экрана:

1. Выделите необходимое соединение в списке и нажмите **Заблокировать**.
2. В открывшемся окне выберите условие блокировки трафика (заблокировать пользователя или IP-адрес источника), отредактируйте при необходимости название правила и опционально установите период действия правила блокировки.
3. Нажмите **Блокировать**.
4. Проверьте созданное правило в разделе правил межсетевого экрана (**Настройки → Политики сети → Межсетевой экран**).

Чтобы создать правило ограничения пропускной способности:

1. Выделите необходимое соединение в списке и нажмите **Ограничить скорость**.
2. В открывшемся окне выберите условие ограничения пропускной способности (ограничить скорость для пользователя или для IP-адреса источника), отредактируйте при необходимости название правила и выберите полосу пропускания.
3. Нажмите **Ограничить скорость**.
4. Проверьте созданное правило в разделе правил пропускной способности (**Настройки → Политики сети → Пропускная способность**).

Маршруты

В разделе **Диагностика и мониторинг → Мониторинг → Маршруты** отображается список всех маршрутов, созданных на узле UserGate SWG.

Вы можете отобразить список маршрутов на одном из узлов кластера или отфильтровать маршруты для определенного виртуального маршрутизатора на узле.

Дополнительно можно отфильтровать вывод списка маршрутов по их типу, нажав **Маршруты**. В фильтре укажите интересующие вас типы маршрутов:

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate SWG. Такие маршруты будут помечены символом **C** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически. Такие маршруты будут помечены символом **K** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Такие маршруты будут помечены символом **O** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Такие маршруты будут помечены символом **B** в списке маршрутов.
- **RIP** — маршруты, полученные по протоколу RIP. Такие маршруты будут помечены символом **R** в списке маршрутов.

Отображаемый список маршрутов можно скачать в виде текстового файла, нажав **Скачать все маршруты**.

OSPF

В разделе **Диагностика и мониторинг → Мониторинг → OSPF** отображается информация о состоянии канала маршрутизации OSPF.

Для выбранного узла кластера и определенного виртуального маршрутизатора на узле вы можете отфильтровать вывод информации по следующим категориям:

- **protocol** — информация о параметрах, необходимых для настройки и функционирования OSPF на маршрутизаторах. (Router ID, области OSPF, маршруты, соседи OSPF, информация о пересылаемых OSPF-сообщениях и состоянии интерфейсов, параметры аутентификации, параметры времени и тайм-аутов).
- **border-routers** — записи таблицы маршрутизации OSPF для пограничного маршрутизатора зоны (ABR) и пограничного маршрутизатора автономной системы (ASBR).
- **database** — информация о состоянии и топологии сети, собранной протоколом OSPF. База данных хранит информацию о маршрутах, соседях, состояниях интерфейсов и других параметрах.
- **route** — информация о всех маршрутах в таблице маршрутизации OSPF.
- **neighbor** — сведения о соседнем маршрутизаторе OSPF для каждого интерфейса. (Neighbor ID, приоритет, состояние, время жизни, интервал простоя, IP-адрес, интерфейс).

Веб-портал

В разделе **Веб-портал** отображается список всех сессий, установленных с веб-порталом UserGate SWG.

Для каждой сессии отображается следующая информация:

- имя пользователя, под которым произошла аутентификация соединения;
- время, когда пользователь подключился к сервису;
- продолжительность соединения;
- IP-адрес пользователя;
- user-agent пользовательского браузера.

Вы можете установить период обновления данных в разделе, выбрав одно из предустановленных значений, или задав его вручную.

Определенные сессии на веб-портале могут быть принудительно закрыты. Для этого:

1. Выделите сессию в списке.
2. Нажмите **Закрыть сессию**.

Сеть

В разделе **Диагностика и мониторинг → Сеть** находятся инструменты для диагностики сетевой связности и обнаружения неисправностей.

Захват пакетов

Сервис захвата пакетов позволяет записывать сетевой трафик в формате PCAP для последующего анализа сетевых проблем.

Чтобы настроить захват трафика:

1. В разделе **Диагностика и мониторинг → Сеть → Захват пакетов** перейдите в блок **Правила**.

2. Нажмите **Добавить**.
3. Создайте правило захвата, указав:
   - название правила;
   - имя файла для записи трафика;
   - максимальный размер файла.

   В качестве дополнительных условий фильтрации в правиле можно указать интерфейсы, на которых будет выполняться захват, и заранее созданные фильтры. В файл будут записываться только пакеты, соответствующие заданным условиям.

Блок **Фильтры** предназначен для настройки условий захвата трафика. Вы можете использовать предустановленные фильтры или создать собственные. При создании фильтра можно указать адрес и порт источника, адрес и порт назначения, а также протокол Ethernet или IPv4. Список доступных протоколов IPv4 приведен по ссылке.

В блоке **Файлы** хранятся записи трафика.

Чтобы начать запись:

1. В блоке **Правила** выберите нужное правило и нажмите **Начать запись**.
2. Для завершения записи нажмите **Остановить запись**.

После завершения захвата созданные файлы отобразятся в блоке **Файлы**.

Запросы в белый список

При блокировке сайтов правилами контентной фильтрации пользователь видит страницу с причиной блокировки. На ней указаны имя сработавшего правила, категория сайта, морфологическая база, черный список, по которому сайт был заблокирован. Если пользователь не согласен с блокировкой, он может прямо с этой страницы отправить запрос на добавление ресурса в белый список, нажав **Добавить в белый список**. Запрос на добавление отобразится на UserGate SWG в разделе **Диагностика и мониторинг → Сеть → Запросы в белый список** .

Для каждого запроса доступны следующие действия:

- **Добавить в белый список** — разрешить доступ к ресурсу.
- **Удалить** — удалить запрос из списка.
- **Отклонить URL** — запретить создание новых запросов для данного URL. При последующих блокировках этого адреса на странице блокировки не будет отображаться кнопка Добавить в белый список.
- **Отклонить домен** — запретить создание новых запросов для всех URL указанного домена. При последующих блокировках ресурсов этого домена кнопка Добавить в белый список отображаться не будет.

Список отклоненных доменов и URL доступен в блоке **Отклоненные запросы**.

Вы можете проверить категорию интернет-ресурса с помощью формы **Проверить URL**. Если сайт отнесен к некорректной категории, можно отправить запрос на ее изменение в UserGate или изменить категорию локально.

Чтобы предложить новую категорию, нажмите **Предложить категорию**. Запрос будет отправлен в компанию UserGate для проверки. Если предложенное изменение будет подтверждено, оно войдет в одно из обновлений базы категорий UserGate URL Filtering.

Для локального изменения категории нажмите **Изменить категорию** и назначьте сайту до двух новых категорий. Просмотреть список сайтов с локально измененными категориями можно в разделе **Настройки → Библиотеки → Измененные категории URL**.

После локального изменения категории при последующих проверках для сайта будут отображаться только назначенные категории, а также специальная категория **Переопределенные пользователем категории**, в которую автоматически включаются все сайты с измененной категоризацией.

Трассировка правил

С помощью трассировки правил вы можете посмотреть, какие правила срабатывают при обработке пользовательских HTTP(S)-запросов. Это может быть полезно при решении проблем с доступом к определенным сайтам.

Чтобы выполнить трассировку правил:

1. В разделе **Диагностика и мониторинг → Сеть → Трассировка правил** нажмите **Настроить** и укажите параметры фильтрации диагностической информации:
   - **Строка** — строка в запросе пользователя, например имя домена, URL, правила контентной фильтрации.
   - **Пользователь** — пользователь, обработку запросов которого необходимо продиагностировать.
   - **IP-адрес источника** — IP-адрес, с которого пользователь выполняет запрос.
   - **IP-адрес назначения** — IP-адрес веб-сервиса, которому направлен запрос.

   Если фильтр не настроен, могут быть отображены результаты обработки запросов других пользователей.
2. Сохраните изменения.
3. Для начала трассировки нажмите **Начать**.
4. Попросите пользователя обратиться к требуемому сайту и посмотрите, какие правила срабатывают при открытии сайта.

   ПримечаниеПри трассировке отображаются сработавшие правила ICAP, инспекции SSL и контентной фильтрации.

Вы можете проверить содержание отображаемого в трассировке интернет-ресурса с помощью формы **Открыть сайт**.

С помощью формы **Добавить в белый список** вы можете поместить выбранный ресурс в один из существующих в системе списков URL.

Ping

С помощью приложения ping вы можете диагностировать доступность сетевых ресурсов путем отправки ICMP Echo Request-пакетов.

Параметры, используемые в приложении ping.

Параметр	Описание
Ping host	IP-адрес или доменное имя узла, доступность которого необходимо проверить
TTL	Значение Time To Live (TTL) для отправляемых пакетов. Определяет максимальное количество маршрутизаторов (переходов), которые пакет может пройти до достижения целевого узла
Интерфейс	IP-адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения команды ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации
Счетчик	Количество ICMP-запросов, которые будут отправлены целевому узлу
Показывать временные метки	Добавление временных меток к строкам вывода для отображения времени отправки и получения пакетов
Не распознавать IP в доменные имена	Отключение обратного DNS-разрешения IP-адресов. В выводе будут отображаться только IP-адреса без преобразования в доменные имена

Traceroute

Приложение traceroute предназначено для определения маршрута прохождения сетевых пакетов до указанного узла и диагностики проблем на отдельных участках сети. В результате выполнения команды отображается список промежуточных маршрутизаторов (переходов) и время отклика для каждого из них.

Параметры, используемые в приложении traceroute.

Параметр	Описание
Traceroute host	IP-адрес или доменное имя узла, до которого необходимо определить маршрут
Использовать ICMP	Выполнение трассировки с использованием ICMP-пакетов. Если параметр не включен, для трассировки используются UDP-пакеты

Параметр	Описание
Интерфейс	Сетевой интерфейс, IP-адрес которого будет использоваться в качестве адреса источника при выполнении трассировки. Маршрут передачи пакетов определяется в соответствии с таблицей маршрутизации
Не распознавать IP в доменные имена	Отключение преобразования IP-адресов промежуточных узлов в доменные имена. В выводе будут отображаться только IP-адреса

Запрос DNS

Приложение «Запрос DNS» предназначено для проверки работоспособности DNS-серверов и корректности разрешения доменных имен. С его помощью вы можете выполнить DNS-запрос заданного типа к указанному DNS-серверу и проанализировать полученный ответ.

Параметры, используемые в приложении «Запрос DNS».

Параметр	Описание
DNS-запрос (хост)	Доменное имя, для которого необходимо выполнить DNS-запрос
IP источника запроса	IP-адрес UserGate SWG, который будет использоваться в качестве адреса источника при отправке DNS-запроса
DNS сервер	IP-адрес DNS-сервера, на который будет отправлен запрос
Порт	Номер UDP-порта, используемого для отправки DNS-запроса. По умолчанию используется порт 53
Тип DNS-запроса	Тип запрашиваемой DNS-записи (A, AXFR, MX, NS)
Тайм-аут ожидания DNS-запросов	Максимальное время ожидания ответа от DNS-сервера. Если в течение указанного интервала ответ не получен, запрос считается завершившимся по тайм-ауту и в результатах отображается соответствующее сообщение об ошибке

LLDP-соседи

В разделе **Диагностика и мониторинг → Сеть → LLDP-соседи** отображается список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. Подробнее о настройке отправки данных по протоколу LLDP — в разделе «Настройка интерфейсов».

ПримечаниеОтображение LLDP-совместимых устройств доступно, только когда в разделе «Настройки» → «Usergate» → «Настройки» включен модуль «Настройка LLDP».

Параметры отображаемых LLDP-совместимых устройств.

Параметр	Описание
Chassis ID	Идентификатор шасси. У каждого устройства UserGate есть только один Chassis ID. В качестве Chassis ID используется MAC-адрес интерфейса управления
SysName	Имя системы
SysDescr	Описание системы, содержит информацию об оборудовании и операционной системе устройства
Management	Адрес соседнего устройства. Содержит информацию: • IP-адрес интерфейса управления (IPv4 и IPv6); • Номер интерфейса для указанного адреса управления
Capability	Функции устройства (например, маршрутизатор, коммутатор и т. п.)
Port ID	Идентификатор порта, с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). В качестве идентификатора используется MAC-адрес интерфейса
PortDescr	Описание порта
TTL	Время жизни передаваемых пакетов LLDP. TTL задается в разделе **UserGate → Настройки → Модули** в поле **Настройка LLDP**

Статистика LLDP

В этом разделе отображается статистика работы протокола LLDP для интерфейсов, на которых настроен и активирован профиль LLDP.

Параметр	Описание
Interface	Название сетевого интерфейса
Transmitted	Общее количество LLDP-кадров, переданных через интерфейс
Received	Общее количество LLDP-кадров, полученных на интерфейсе.
Discarded	Количество полученных LLDP-кадров, которые были отброшены в результате ошибок обработки или несоответствия формату протокола
Unrecognized	Количество полученных LLDP-кадров, содержащих неизвестные или неподдерживаемые TLV-элементы
Ageout	Количество записей о LLDP-соседях, удаленных после истечения срока действия информации. Если в течение времени жизни, указанного в LLDP-объявлении, от соседа не поступают новые LLDP-кадры, соответствующая запись автоматически удаляется
Inserted	Количество записей о LLDP-соседях, добавленных в таблицу соседей LLDP
Deleted	Количество записей о LLDP-соседях, удаленных из таблицы соседей LLDP

Мониторинг состояния устройства по протоколу SNMP

Documentation: ☑
Product: SWG
Version: 7.5.x

UserGate SWG поддерживает мониторинг состояния устройства по протоколу SNMP версий 2c и 3.

Корпоративные системы мониторинга могут получать информацию о состоянии UserGate SWG посредством SNMP-запросов (SNMP queries), а также принимать SNMP-уведомления (SNMP traps), отправляемые устройством при возникновении определенных событий.

Настройка мониторинга UserGate SWG с помощью SNMP

Чтобы настроить мониторинг UserGate SWG с помощью SNMP:

1. Настройте общие параметры SNMP-агента UserGate SWG.
2. Откройте доступ к сервису SNMP в параметрах контроля доступа зоны интерфейса, через который будет выполняться подключение по протоколу SNMP. Подробнее о настройке параметров зон — в разделе « Настройка зон».
3. Настройте профили безопасности SNMP на UserGate SWG для подключения к нему корпоративных SNMP-менеджеров (только для протокола SNMP v3).
4. Создайте правила SNMP для управления мониторингом устройства.

Настроить мониторинг можно двумя способами: в веб-консоли устройства или в интерфейсе командной строки (CLI).

Общие параметры SNMP-агента UserGate SWG

Настройка в веб-консоли

Чтобы настроить общие параметры SNMP-агента в веб-консоли UserGate SWG:

1. В разделе **Диагностика и мониторинг → Оповещения → Параметры SNMP** выделите строку с параметрами устройства и нажмите **Редактировать**.
2. Отредактируйте параметры SNMP-агента.

Параметр	Описание
SNMP-имя системы	Название системы, используемое SNMP-агентом
SNMP-локация системы	Информация о физическом расположении системы
SNMP-описание системы	Произвольное описание системы
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. Вы можете создать собственный идентификатор узла, указав значения следующих параметров: • **Тип**; • **Длина**; • **Значение идентификатора**. Идентификатор может быть одного из следующих типов: • IPv4 (**ip4**); • IPv6 (**ipv6**); • MAC-адрес (**mac**); • текст (**text**); • октеты (**octets**). Длина идентификатора может быть определена как **фиксированная** (не более 8 байт) или **динамическая** (не более 27 байт). Фиксированная длина идентификатора применима только для типа **текст**

Настройка в CLI

В интерфейсе командной строки UserGate SWG общие параметры SNMP-агента настраиваются на уровне monitoring snmp-parameter.

Для настройки общих параметров используется команда:

Admin@nodename# set monitoring snmp-parameter {node-name} <parameters>

Укажите в команде значения соответствующих параметров.

Параметр	Описание
agent-name	Название системы, используемое SNMP-агентом
location	Информация о физическом расположении SNMP-агента
description	Произвольное описание системы
Engine ID: • ip4; • ip6; • mac; • text; • octets	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. Вы можете создать собственный идентификатор узла, указав значения следующих параметров: • тип; • длина; • значение идентификатора. Идентификатор может быть одного из следующих типов: • IPv4 (ip4); • IPv6 (ipv6); • MAC-адрес (mac); • текст (text); • октеты (octets). Длина идентификатора (length) может быть фиксированной (fixed, не более 8 байт) или динамической (dynamic, не более 27 байт). Фиксированная длина идентификатора применима только для типа text

Команда для просмотра значений общих параметров SNMP-агента:

Admin@nodename# show monitoring snmp-parameter

Пример настройки общих параметров SNMP-агента в CLI:

```
Admin@nodename# set monitoring snmp-parameter utmcore@nodename agent-name "SWG1" description "Optional description" location "Test location" ip4 10.10.0.10 length dynamic
Admin@nodename# show monitoring snmp-parameter

status          : online
agent-name      : SWG1
```

description : Optional description
location : Test location
length : dynamic
ip4 : 10.10.0.10

Профили безопасности SNMP

Для подключения SNMP-менеджера к UserGate SWG по протоколу SNMP v3 создайте профиль безопасности SNMP и укажите в нем параметры аутентификации и шифрования.

ПримечаниеЗначения параметров аутентификации для SNMP v3 должны совпадать на SNMP-менеджере и в профиле безопасности SNMP на UserGate SWG.

Информацию о настройке аутентификации для вашего SNMP-менеджера смотрите в руководстве к используемому ПО для управления по SNMP.

Настройка в веб-консоли

Чтобы создать профиль безопасности SNMP в веб-консоли UserGate SWG:

1. В разделе **Диагностика и мониторинг → Оповещения → Профили безопасности SNMP** нажмите **Добавить**.
2. Заполните параметры профиля.

Параметр	Описание
Название	Название профиля безопасности SNMP
Описание	Произвольное описание профиля
Пользователь	Имя пользователя, используемое SNMP-менеджером для аутентификации
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера: • Без аутентификации и шифрования. • С аутентификацией, без шифрования. • С аутентификацией и шифрованием. Рекомендуется использовать последний режим аутентификации, обеспечивающий максимальный уровень защиты
Алгоритм аутентификации	Алгоритм проверки подлинности пользователя: • **SHA1**; • **MD5**; • **SHA224**; • **SHA256**; • **SHA384**; • **SHA512**
Пароль аутентификации	Пароль, используемый для аутентификации
Алгоритм шифрования	Алгоритм шифрования данных: • **DES**; • **AES**
Пароль шифрования	Пароль, используемый для шифрования данных

Настройка в CLI

В интерфейсе командной строки UserGate SWG профили безопасности SNMP создаются на уровне monitoring snmp-security-profile.

Для создания профиля безопасности SNMP используется команда:

Admin@nodename# create monitoring snmp-security-profile <parameters>

Укажите в команде значения соответствующих параметров.

Параметр	Описание
name	Название профиля безопасности SNMP
description	Произвольное описание профиля безопасности SNMP
username	Имя пользователя для аутентификации SNMP-менеджера
auth-type	Режим аутентификации SNMP-менеджера: • none — без аутентификации, без шифрования. • no-encrypt — с аутентификацией, без шифрования. • encrypt — с аутентификацией, с шифрованием. Рекомендуется использовать режим аутентификации encrypt, обеспечивающий максимальный уровень защиты
auth-alg	Алгоритм проверки подлинности пользователя: • sha; • md5; • sha224; • sha256; • sha384; • sha512
auth-password	Пароль, используемый для аутентификации
encrypt-alg	Алгоритм, используемый для шифрования данных: • des; • aes
encrypt-password	Пароль, используемый для шифрования данных

Команда для изменения существующего профиля безопасности SNMP:

Admin@nodename# set monitoring snmp-security-profile {profile-name} <parameters>

Команда для просмотра созданного ранее профиля безопасности SNMP:

Admin@nodename# show monitoring snmp-security-profile {profile-name}

Команда для удаления созданного ранее профиля безопасности SNMP:

Admin@nodename# delete monitoring snmp-security-profile {profile-name}

Пример создания профиля безопасности SNMP в CLI:

```
Admin@nodename# create monitoring snmp-security-profile name "Profile 1" description "Optional description" username test_user auth-type encrypt auth-alg sha256 auth-password 12345678 encrypt-alg aes encrypt-password 87654321
Admin@nodename# show monitoring snmp-security-profile "Profile 1"

name          : Profile 1
description   : Optional description
username      : test_user
auth-type     : encrypt
auth-alg      : sha256
encrypt-alg   : aes
```

Правила SNMP

С помощью правил SNMP вы можете управлять параметрами мониторинга устройства:

- выбирать версию протокола SNMP;
- устанавливать способы получения данных;
- определять список отслеживаемых показателей.

Настройка в веб-консоли

Чтобы создать правило SNMP в веб-консоли UserGate SWG:

1. В разделе **Диагностика и мониторинг → Оповещения → SNMP** нажмите **Добавить**.
2. Укажите значения параметров правила.

Параметр	Описание
Название правила	Название правила
IP-адрес сервера для трапов	IP-адрес сервера для получения уведомлений и порт, на котором сервер слушает уведомления. Обычно это порт UDP 162. Параметр указывается только в случае, если выбран способ получения информации об устройстве с помощью уведомлений (SNMP traps)
Комьюнити	SNMP community — строка для идентификации UserGate NGFW и системы мониторинга для протокола SNMP v2c. При указании названия SNMP community используйте только латинские буквы или цифры
Контекст	Опциональный параметр, определяющий SNMP context. Можно использовать только латинские буквы или цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию
Версия	Версия протокола SNMP, которая будет использоваться в этом правиле (SNMP v2c или SNMP v3)
Разрешить SNMP-запросы	При включении параметра разрешается получение и обработка SNMP-запросов от SNMP-менеджера
Разрешить SNMP-трапы	При включении параметра разрешается отправка SNMP-уведомлений на сервер, настроенный для приема оповещений
Название профиля безопасности SNMP	Выбор профиля безопасности SNMP для подключения корпоративной системы мониторинга к UserGate NGFW (только для протокола SNMP v3)
События	Выбор типов параметров, доступных для мониторинга по правилу

Настройка в CLI

В интерфейсе командной строки UserGate SWG правила SNMP создаются на уровне monitoring snmp.

Для создания правила SNMP используется команда:

Admin@nodename# create monitoring snmp <parameters>

Укажите в команде значения соответствующих параметров.

Параметр	Описание
name	Название правила
enabled	Включение или отключение правила
community	SNMP community — строка для идентификации UserGate NGFW и системы мониторинга для протокола SNMP v2c. При указании названия SNMP community используйте только латинские буквы или цифры
context	Опциональный параметр, определяющий SNMP context. Можно использовать только латинские буквы или цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию
version	Версия протокола SNMP, которая будет использоваться в этом правиле: • 2 — SNMP v2c; • 3 — SNMP v3
query	При включении параметра разрешается получение и обработка SNMP-запросов от SNMP-менеджера
trap	При включении параметра разрешается отправка SNMP-уведомлений на сервер, настроенный для приема оповещений

Параметр	Описание
trap-host	IP-адрес сервера для отправки SNMP-уведомлений (SNMP traps)
trap-port	Порт, на котором сервер слушает SNMP-уведомления. Обычно это порт UDP 162
security-profile	Профиль безопасности SNMP (только для протокола SNMP v3)
events	Выбор типов параметров, доступных для мониторинга по правилу

Команда для изменения существующего правила SNMP:

Admin@nodename# set monitoring snmp {rule-name} <parameters>

Команда для просмотра созданного ранее правила SNMP:

Admin@nodename# show monitoring snmp {rule-name}

Команда для удаления созданного ранее правила SNMP:

Admin@nodename# delete monitoring snmp {rule-name}

Пример создания правила SNMP в CLI:

Admin@nodename# create monitoring snmp name "Rule 1" description "Test rule" version 2 community test1 query on trap on trap-host 10.10.0.100 trap-port 162 events [ha-status-changed ha-member-up ha-member-down license-information] er
Admin@nodename# show monitoring snmp "Rule 1"

```
name              : Rule 1
description       : Test rule
enabled           : on
community         : test1
version           : 2
security-profile  : none
query             : on
trap              : on
trap-host         : 10.10.0.100
trap-port         : 162
events            : ha-status-changed; ha-member-up; ha-member-down; license-information
```

Оповещения

С помощью механизма оповещений вы можете настроить автоматическое информирование администраторов устройства о возникновении различных событий по SMS или электронной почте.

Для настройки оповещений:

1. Создайте профиль оповещения. Подробнее — в разделе « Профили оповещений».
2. Создайте группу получателей оповещений. Подробнее — в разделах « Почтовые адреса» и «Номера телефонов».
3. Создайте правило оповещения.

Правила оповещений

Вы можете создавать правила оповещений как в веб-консоли устройства, так и в интерфейсе командной строки (CLI).

Настройка в веб-консоли

Чтобы создать правило оповещения в веб-консоли UserGate SWG:

1. В разделе **Диагностика и мониторинг → Оповещения → Правила оповещений** , нажмите **Добавить**.
2. Укажите значения параметров правила.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Описание	Произвольное описание правила
Профиль оповещения	Выбор или создание профилей оповещения. Для профилей SMPP доступна вкладка **Телефоны**, в которой необходимо указать списки телефонных номеров адресатов. Для профилей SMTP доступна вкладка **Emails**, в которой необходимо указать списки email-адресов адресатов
От	Указание отправителя оповещения
Тема	Тема оповещения (для профилей SMTP)
Тайм-аут перед повторной отправкой (сек.)	Интервал, в течение которого устройство не будет отправлять сообщение при повторном срабатывании этого правила. Параметр позволяет предотвратить шторм сообщений при частом срабатывании правила
События	Выбор событий, для которых необходимо отправлять оповещения
Телефоны	Списки номеров телефонов для отправки SMS-оповещений (для профилей SMPP)
Emails	Списки email-адресов для отправки почтовых оповещений (для профилей SMTP)

Настройка в CLI

В интерфейсе командной строки правила оповещений создаются на уровне monitoring alert-rules.

Для создания правила оповещения используется команда:

Admin@nodename# create monitoring alert-rules <parameters>

Укажите в команде значения соответствующих параметров.

Параметр	Описание
enabled	Включение или отключение правила
name	Название правила
description	Произвольное описание правила

Параметр	Описание
notification-profile	Созданный ранее профиль оповещения (SMPP или SMTP)
sender	Отправитель оповещения
subject	Тема оповещения (для профилей SMTP)
timeout	Интервал, в течение которого устройство не будет отправлять сообщение при повторном срабатывании этого правила. Параметр позволяет предотвратить шторм сообщений при частом срабатывании правила
events	События, для которых необходимо отправлять оповещения
phones	Списки номеров телефонов для отправки SMS-оповещений (для профилей SMPP)
emails	Списки email-адресов для отправки почтовых оповещений (для профилей SMTP)

Команда для изменения существующего правила оповещения:

Admin@nodename# set monitoring alert-rules {alert-rule-name} <parameters>

Команда для просмотра созданного ранее правила оповещения:

Admin@nodename# show monitoring alert-rules {alert-rule-name}

Команда для удаления созданного ранее правила оповещения:

Admin@nodename# delete monitoring alert-rules {alert-rule-name}

Пример создания правила оповещения в CLI:

Admin@nodename# create monitoring alert-rules name "Alert rule 1" description "Test alert rule" notification-profile "Example SMTP profile" emails [Email_list1] sender test@test.com subject "Test alert" timeout 60 events [ha-status-changed ha-m
Admin@nodename# show monitoring alert-rules "Alert rule 1"

name : Alert rule 1
description : Test alert rule
enabled : on
timeout : 60
notification-profile : Example SMTP profile
emails : Email_list1
subject : Test alert
events : ha-status-changed; ha-member-up; ha-member-down
sender : test@test.com

MIB-файлы

Для получения доступа к информации, специфичной для устройств UserGate, необходимо добавить в базу данных вашего SNMP-менеджера MIB-файлы UserGate.

Чтобы скачать актуальные MIB-файлы из веб-консоли устройства UserGate:

Перейдите в раздел **Диагностика и мониторинг → Оповещения → SNMP** и нажмите **Скачать MIB**.

В ZIP-архиве находятся следующие MIB-файлы:

- UTM-ENTERPRISE-MIB;
- UTM-MIB;
- UTM-INTERFACES-MIB;
- UTM-TEMPERATURE-MIB;
- UTM-TRAPS-MIB;
- UTM-TRAPS-BINDINGS-MIB.

MIB-файлы содержат как проприетарные, так и стандартные параметры, используемые для мониторинга устройств UserGate.

Уникальный идентификатор SNMP PEN (private enterprise number) компании UseGate: 45741.

UTM-MIB

Файл содержит таблицы проприетарных параметров мониторинга состояния устройств UserGate.

OID	Наименование	Тип данных	Описание
1.3.6.1.4.1.45741.2.2	utmInfo	sequence	Раздел частной информации UserGate
1.3.6.1.4.1.45741.2.2.1	utmInfoEntities	sequence	Таблицы частных параметров UserGate
1.3.6.1.4.1.45741.2.2.1.1	systemInfo	sequence	Таблица с системной информацией
1.3.6.1.4.1.45741.2.2.1.1.1	vcpuCount	integer	Количество виртуальных процессоров в системе
1.3.6.1.4.1.45741.2.2.1.1.2	vcpuUsage	integer	Загруженность виртуальных процессоров системы. Отображается фактическое число загруженных виртуальных процессоров
1.3.6.1.4.1.45741.2.2.1.1.3	usersCounter	integer	Количество активных пользователей на текущий момент времени
1.3.6.1.4.1.45741.2.2.1.1.4	sessionsCounter	integer	Количество активных сессий на текущий момент времени
1.3.6.1.4.1.45741.2.2.1.1.5	tcpsessionsCounter	integer	Количество активных TCP-сессий на текущий момент времени
1.3.6.1.4.1.45741.2.2.1.1.6	udpsessionsCounter	integer	Количество активных UDP-сессий на текущий момент времени
1.3.6.1.4.1.45741.2.2.1.1.7	icmpsessionsCounter	integer	Количество активных ICMP-сессий на текущий момент времени
1.3.6.1.4.1.45741.2.2.1.1.8	sessionsRate10	integer	Количество новых сессий в секунду. Среднее значение за последние 10 секунд
1.3.6.1.4.1.45741.2.2.1.1.9	sessionsRate60	integer	Количество новых сессий в секунду. Среднее значение за последние 60 секунд
1.3.6.1.4.1.45741.2.2.1.1.10	sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд
1.3.6.1.4.1.45741.2.2.1.1.11	tcpsessionsRate10	integer	Количество новых TCP-сессий в секунду. Среднее значение за последние 10 секунд
1.3.6.1.4.1.45741.2.2.1.1.12	tcpsessionsRate60	integer	Количество новых TCP-сессий в секунду. Среднее значение за последние 60 секунд

OID	Наименование	Тип данных	Описание
1.3.6.1.4.1.45741.2.2.1.1.13	tcpsessionsRate300	integer	Количество новых TCP-сессий в секунду. Среднее значение за последние 300 секунд
1.3.6.1.4.1.45741.2.2.1.1.14	udpsessionsRate10	integer	Количество новых UPD-сессий в секунду. Среднее значение за последние 10 секунд
1.3.6.1.4.1.45741.2.2.1.1.15	udpsessionsRate60	integer	Количество новых UPD-сессий в секунду. Среднее значение за последние 60 секунд
1.3.6.1.4.1.45741.2.2.1.1.16	udpsessionsRate300	integer	Количество новых UPD-сессий в секунду. Среднее значение за последние 300 секунд
1.3.6.1.4.1.45741.2.2.1.1.17	icmpsessionsRate10	integer	Количество новых ICMP-сессий в секунду. Среднее значение за последние 10 секунд
1.3.6.1.4.1.45741.2.2.1.1.18	icmpsessionsRate60	integer	Количество новых ICMP-сессий в секунду. Среднее значение за последние 60 секунд
1.3.6.1.4.1.45741.2.2.1.1.19	icmpsessionsRate300	integer	Количество новых ICMP-сессий в секунду. Среднее значение за последние 300 секунд
1.3.6.1.4.1.45741.2.2.1.1.20	dnsRequestCounter	integer	Общее количество DNS-запросов
1.3.6.1.4.1.45741.2.2.1.1.21	dnsBlockedRequestCounter	integer	Количество заблокированных DNS-запросов
1.3.6.1.4.1.45741.2.2.1.1.22	dnsRequestRate	integer	Количество DNS-запросов в секунду
1.3.6.1.4.1.45741.2.2.1.1.23	httpRequestCounter	integer	Общее количество HTTP-запросов
1.3.6.1.4.1.45741.2.2.1.1.24	httpBlockedRequestCounter	integer	Количество заблокированных HTTP-запросов
1.3.6.1.4.1.45741.2.2.1.1.25	httpRequestRate	integer	Количество HTTP-запросов в секунду
1.3.6.1.4.1.45741.2.2.1.1.26	dataPartitionFSStatus	string	Состояние файловой системы: • clean — нормальное состояние; • not_clean — требуется проверка файловой системы
1.3.6.1.4.1.45741.2.2.1.2	haClusterInfo	sequence	Таблица информации о кластере
1.3.6.1.4.1.45741.2.2.1.2.1	haStatus	integer	Текущий статус узла кластера отказоустойчивости: • 0 — мастер-узел; • 1 — резервный узел; • 3 — ошибка
1.3.6.1.4.1.45741.2.2.1.3	idpsInfo	sequence	Таблица информации о системе СОВ
1.3.6.1.4.1.45741.2.2.1.4	deviceInfo	sequence	Таблица информации о ПАК
1.3.6.1.4.1.45741.2.2.1.4.1	cpuLoad	integer	Загруженность центрального процессора системы, %.
1.3.6.1.4.1.45741.2.2.1.4.2	memoryUsed	integer	Использование оперативной памяти, %.
1.3.6.1.4.1.45741.2.2.1.4.3	logDiskSpace	integer	Пространство на диске, используемое под журналы, %.
1.3.6.1.4.1.45741.2.2.1.4.4	powerSupply1Status	string	Состояние первого источника питания: • no_power_supplies; • on — включен; • off — отключен
1.3.6.1.4.1.45741.2.2.1.4.5	powerSupply2Status	string	Состояние второго источника питания: • no_power_supplies; • on — включен; • off — отключен
1.3.6.1.4.1.45741.2.2.1.4.6	raidType	string	Тип RAID массива
1.3.6.1.4.1.45741.2.2.1.4.7	raidStatus	string	Текущий статус RAID (Redundant Array of Independent Disks): • no_raid; • 0 — optimal, массив в оптимальном состоянии; • 1 — degraded, полный или частичный выход из строя одного из дисков; • 2 — rebuild, восстановление массива
1.3.6.1.4.1.45741.2.2.1.4.8	diskIOUtilization	integer	Текущая утилизация диска (%)
1.3.6.1.4.1.45741.2.2.1.4.9	diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд
1.3.6.1.4.1.45741.2.2.1.4.10	diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд

UTM-INTERFACES-MIB

Файл содержит набор параметров мониторинга состояния интерфейсов из стандартных баз RFC1213-MIB и IF-MIB, используемых в устройствах UserGate.

OID	Наименование	Тип данных	Описание
1.3.6.1.2.1.2.1.0	ifNumber	integer	Количество сетевых интерфейсов
1.3.6.1.2.1.2.2	ifTable	sequence	Таблица информации о сетевых интерфейсах

OID	Наименование	Тип данных	Описание
1.3.6.1.2.1.2.2.1	ifEntry	sequence	Информация об интерфейсе
1.3.6.1.2.1.2.2.1.1.A	ifIndex	integer	Индекс сетевого интерфейса (A). Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber
1.3.6.1.2.1.2.2.1.2.A	ifDescr	string	Информация об интерфейсе, которая может включать в себя название производителя, имя продукта, аппаратную версию интерфейса
1.3.6.1.2.1.2.2.1.3.A	ifType	integer	Тип интерфейса, определенный в соответствии с протоколом физического или канального уровней: • 1 — other, неизвестный тип; • 2 — regular1822, определен в BBN Report 1822; • 3 — hdh1822, определен в BBN Report 1822; • 4 — ddn-x25, определен в BBN Report 1822; • 5 — rfc877-x25, определен в стандарте канального уровня сетевой модели OSI X.25; • 6 — ethernet-csmacd, сетевой интерфейс типа Ethernet, независимо от скорости (определен в RFC 3635); • 7 — iso88023-csmacd, определен в IEEE 802.3; • 8 — iso88024-tokenBus, определен в стандарте IEEE 8802.4; • 9 — iso88025-tokenRing, сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5; • 10 — iso88026-man, определен в стандарте ISO 88026 "MAN"; • 11 — starLan, определен в стандарте IEEE 802.3e; • 12 — proteon-10Mbit, Proteon 10 Mbit; • 13 — proteon-80Mbit, Proteon 80 Mbit; • 14 — hyperchannel, высокоскоростной канал, используемы в сети ISDN; • 15 — fddi, сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети; • 16 — lapb, протокол канального уровня, используемым для передачи пакетов стандарта X.25; • 17 — sdlc, протокол канального уровня для системной сетевой архитектуры IBM; • 18 — ds1, способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1; • 19 — e1, европейский аналог T1; • 20 — basicISDN, для связи аппаратуры абонента и ISDN-станции; • 21 — primaryISDN, используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы; • 22 — propPointToPointSerial, определен в стандарте RFC1213; • 23 — ppp, сетевой интерфейс использует подключение PPP (Point-To-Point Protocol); • 24 — softwareLoopback, сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть; • 25 — eon, ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определен в ISO/IEC 8473-1; • 26 — ethernet-3Mbit, сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895; • 27 — nsip, XNS over IP — предназначен для использования в разнообразных средах передачи данных; • 28 — slip, сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055; • 29 — ultra, ULTRA Technologies; • 30 — ds3, высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3; • 31 — sip, сетевой интерфейс использует протокол для высокоскоростной передачи данных SMDS (Switched Multimegabit Data Service). SMDS определяется в стандарте IETF RFC 1694; • 32 — frame-relay, обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети
1.3.6.1.2.1.2.2.1.4.A	ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно переслать через этот интерфейс
1.3.6.1.2.1.2.2.1.5.A	ifSpeed	gauge32	Пропускная способность интерфейса (бит/с). Максимальное значение: 4 294 967 295 (≈ 4,29 Гбит/с). Рекомендуется использовать для интерфейсов со скоростью до 4,29 Гбит/с, когда требуется высокая точность
1.3.6.1.2.1.2.2.1.6.A	ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес)
1.3.6.1.2.1.2.2.1.7.A	ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: • 1 — up, готов для передачи пакетов; • 2 — down, не работает; • 3 — testing, в режиме тестирования; рабочие пакеты не могут быть переданы
1.3.6.1.2.1.2.2.1.8.A	ifOperStatus	integer	Текущий статус работы интерфейса: • 1 — up, интерфейс готов для передачи пакетов; • 2 — down, интерфейс не может передавать пакеты данных; • 3 — testing, выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы; • 4 — unknown, интерфейс находится в неизвестном состоянии; • 5 — dormant, сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие; • 6 — notPresent, сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного; • 7 — lowerLayerDown, передача пакетов через интерфейс невозможна, так как один или несколько используемых им интерфейсов нижнего уровня недоступны или находятся в состоянии отказа
1.3.6.1.2.1.2.2.1.9.A	ifLastChange	timeticks	Значение SysUpTime на момент перехода интерфейса в данное состояние
1.3.6.1.2.1.2.2.1.10.A	ifInOctets	counter32	Количество байтов, принятое интерфейсом, включая служебные
1.3.6.1.2.1.2.2.1.11.A	ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки
1.3.6.1.2.1.2.2.1.12.A	ifInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов

OID	Наименование	Тип данных	Описание
1.3.6.1.2.1.2.2.1.13.A	ifInDiscards	counter32	Количество входящих пакетов, отброшенных несмотря на отсутствие ошибок, препятствующих их обработке или доставке. Одной из возможных причин отбрасывания является нехватка или освобождение буферной памяти.
1.3.6.1.2.1.2.2.1.14.A	ifInErrors	counter32	Количество входящих пакетов с ошибками, препятствующими их корректной обработке и доставке
1.3.6.1.2.1.2.2.1.15.A	ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола
1.3.6.1.2.1.2.2.1.16.A	ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные
1.3.6.1.2.1.2.2.1.17.A	ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены
1.3.6.1.2.1.2.2.1.18.A	ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены
1.3.6.1.2.1.2.2.1.19.A	ifOutDiscards	counter32	Количество исходящих пакетов, отброшенных несмотря на отсутствие ошибок, препятствующих их передаче. Одной из возможных причин отбрасывания является недостаток доступного буферного пространства
1.3.6.1.2.1.2.2.1.20.A	ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок
1.3.6.1.2.1.2.2.1.21.A	ifOutQLen	gauge32	Длина выходной очереди (в пакетах)
1.3.6.1.2.1.4.20	ipAddrTable	sequence	Таблица адресной информации интерфейсов
1.3.6.1.2.1.4.20.1	ipAddrEntry	sequence	Информация об адресах интерфейсов
1.3.6.1.2.1.4.20.1.1.L.B	ipAdEntAddr	IpAddress	IP-адрес интерфейса, L — длина в байтах, B — значение
1.3.6.1.2.1.4.20.1.2.L.B	ipAdEntIfIndex	integer	Индекс интерфейса, к которому привязан данный IP-адрес (из таблицы 1.3.6.1.2.1.2.2.1)
1.3.6.1.2.1.4.20.1.3.L.B	ipAdEntNetMask	IpAddress	Маска подсети интерфейса
1.3.6.1.2.1.4.20.1.4L.B	ipAdEntBcastAddr	integer	Широковещательный адрес интерфейса
1.3.6.1.2.1.4.20.1.5.L.B	ipAdEntReasmMaxSize	integer	Максимальный размер IP-датаграммы, собранной из фрагментов
1.3.6.1.2.1.31.1.1	ifXTable	sequence	Таблица информации об интерфейсах
1.3.6.1.2.1.31.1.1.1	ifXEntry	sequence	Информация об интерфейсе
1.3.6.1.2.1.31.1.1.1.1.L.X.Y.Z	ifName	string	Название интерфейса, используемое в системе. L — длина в символах, X.Y.Z — коды символов
1.3.6.1.2.1.31.1.1.1.2.L.X.Y.Z	ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки
1.3.6.1.2.1.31.1.1.1.3.L.X.Y.Z	ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов
1.3.6.1.2.1.31.1.1.1.4.L.X.Y.Z	ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены
1.3.6.1.2.1.31.1.1.1.5.L.X.Y.Z	ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены
1.3.6.1.2.1.31.1.1.1.6.L.X.Y.Z	ifHCInOctets	counter64	Параметр, аналогичный ifInOctets — количество байтов, принятое данным интерфейсом, включая служебные; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.7.L.X.Y.Z	ifHCInUcastPkts	counter64	Параметр, аналогичный ifInUcastPkts — количество доставленных пакетов одноадресной рассылки; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.8.L.X.Y.Z	ifHCInMulticastPkts	counter64	Параметр, аналогичный ifInMulticastPkts — количество доставленных пакетов многоадресной рассылки; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.9.L.X.Y.Z	ifHCInBroadcastPkts	counter64	Параметр, аналогичный ifInBroadcastPkts — количество доставленных широковещательных пакетов; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.10.L.X.Y.Z	ifHCOutOctets	counter64	Параметр, аналогичный ifOutOctets — количество байтов, переданное данным интерфейсом, включая служебные; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.11.L.X.Y.Z	ifHCOutUcastPkts	counter64	Параметр, аналогичный ifOutUcastPkts — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.12.L.X.Y.Z	ifHCOutMulticastPkts	counter64	Параметр, аналогичный ifOutMulticastPkts — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.13.L.X.Y.Z	ifHCOutBroadcastPkts	counter64	Параметр, аналогичный ifOutBroadcastPkts — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
1.3.6.1.2.1.31.1.1.1.14.L.X.Y.Z	ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • 1 — enabled, включено; • 2 — disabled, отключено
1.3.6.1.2.1.31.1.1.1.15.L.X.Y.Z	ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в Мбит/с. Округление до целых Мбит/с (теряется точность для скоростей < 1 Мбит/с). Рекомендуется применять для высокоскоростных интерфейсов
1.3.6.1.2.1.31.1.1.1.16.L.X.Y.Z	ifPromiscuousMode	integer	«Неразборчивый режим». Возможные значения: • 1 — true, узел принимает все пакеты независимо от того, кому они адресованы; • 2 — false, интерфейс принимает только пакеты, адресованные этому узлу; Значение параметра не влияет на прием широковещательных и многоадресных пакетов
1.3.6.1.2.1.31.1.1.1.17.L.X.Y.Z	ifAlias	string	Название интерфейса, заданное администратором при настройке
1.3.6.1.2.1.31.1.1.1.18.L.X.Y.Z	ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счетчиков интерфейса

UTM-TEMPERATURE-MIB

Файл содержит таблицу проприетарных параметров мониторинга температуры для устройств UserGate.

Данные температурных сенсоров отображаются только для поддерживаемых аппаратных платформ. В настоящее время поддерживаются ПАК UserGate C150 и FG.

Для неподдерживаемых платформ или виртуальных решений таблица сенсоров будет пустой, а значения количества сенсоров и пределы рабочих температур будут равны нулю.

OID	Наименование	Тип данных	Описание
1.3.6.1.4.1.45741.2.2.1.7	temperatureInfo	sequence	Таблица информации о температуре
1.3.6.1.4.1.45741.2.2.1.7.1	thermNumber	integer	Количество температурных сенсоров на данной платформе
1.3.6.1.4.1.45741.2.2.1.7.2	thermLowerThreshold	integer	Нижний предел рабочей температуры
1.3.6.1.4.1.45741.2.2.1.7.3	thermUpperThreshold	integer	Верхний предел рабочей температуры
1.3.6.1.4.1.45741.2.2.1.7.4	thermTable	sequence	Таблица температурных сенсоров с показаниями (thermEntry)
1.3.6.1.4.1.45741.2.2.1.7.4.1	thermEntry	sequence	Информация о конкретном сенсоре: • thermName (string) — название сенсора; • thermValue (integer) — показание сенсора; • thermUnit (string) — единица измерения показаний сенсора

ПримечаниеСенсоры, с которых не удалось получить показания температуры, не отображаются в таблице. При этом параметр thermNumber учитывает все температурные сенсоры, включая неработающие, поэтому его значение может не совпадать с количеством записей в таблице.

UTM-TRAPS-MIB

Файл содержит описание проприетарных параметров, используемых в SNMP-уведомлениях (traps) о состоянии устройств UserGate.

OID	Наименование	Описание	Передаваемые параметры (по таблице UTM-TRAPS-BINDINGS-MIB)
1.3.6.1.4.1.45741.2.10	utmTraps	Раздел специфических оповещений UserGate	
1.3.6.1.4.1.45741.2.10.1	utmTrapsEntities	Таблицы специфических оповещений UserGate	
1.3.6.1.4.1.45741.2.10.1.1	utmSysInfoEntities	Таблица системных оповещений	
1.3.6.1.4.1.45741.2.10.1.1.1	trapCoreCrush	Сбой ядра	
1.3.6.1.4.1.45741.2.10.1.1.2	trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен	
1.3.6.1.4.1.45741.2.10.1.1.3	trapCoreBootstrapEnd	Загрузка сервера завершена успешно	
1.3.6.1.4.1.45741.2.10.1.1.4	trapDefaultGatewayChanged	Изменение шлюза по умолчанию	
1.3.6.1.4.1.45741.2.10.1.1.5	trapHighSessionsCounter	Таблица сессий заполнена на 90%	utmSessions; utmSessionsMax
1.3.6.1.4.1.45741.2.10.1.1.6	trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии	utmUsers; utmUsersMax
1.3.6.1.4.1.45741.2.10.1.1.7	trapDataPartitionFSStatus	Статус файловой системы. Состояние файловой системы изменилось на not_clean	utmDataPartionFSStatus
1.3.6.1.4.1.45741.2.10.1.2	utmHAClusterEntities	Таблица оповещений кластера	
1.3.6.1.4.1.45741.2.10.1.2.1	trapStatusChanged	Изменение статуса узла отказоустойчивого кластера	utmHAStatus; utmHAStatusReason
1.3.6.1.4.1.45741.2.10.1.2.2	trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен»	Значение SysUpTime, когда статус узла отказоустойчивого кластера изменился на «Подключен»
1.3.6.1.4.1.45741.2.10.1.2.3	trapMemberDown	Узел отказоустойчивого кластера отключен	Значение SysUpTime, когда статус узла отказоустойчивого кластера изменился на «Отключен»
1.3.6.1.4.1.45741.2.10.1.3	utmIDPSEntities	Таблица оповещений СОВ	
1.3.6.1.4.1.45741.2.10.1.3.1	trapAttackDetected	Обнаружение атаки системой СОВ	Значение SysUpTime, когда произошло обнаружение атаки системой СОВ
1.3.6.1.4.1.45741.2.10.1.4	utmDeviceEntities	Таблица оповещений оборудования	
1.3.6.1.4.1.45741.2.10.1.4.1	trapChecksumFailed	Нарушение целостности бинарных файлов	
1.3.6.1.4.1.45741.2.10.1.4.2	trapHighCPUUsage	Высокая загрузка центрального процессора (95%)	utmCPUUsage
1.3.6.1.4.1.45741.2.10.1.4.3	trapLowMemory	Высокая загрузка памяти (95%)	utmMemory
1.3.6.1.4.1.45741.2.10.1.4.4	trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов	utmLogdiskSpace
1.3.6.1.4.1.45741.2.10.1.4.5	trapRaidStatus	Изменение статуса RAID	utmAdaptecRaidStatus; utmBroadcomRaidStatus
1.3.6.1.4.1.45741.2.10.1.4.6	trapPowerSupply	Первый источник питания отключен	utmPowerSupply; utmPowerSupplyStatus
1.3.6.1.4.1.45741.2.10.1.4.7	trapCableStatus	Кабель был подключен или отключен от интерфейса	utmCSCIfName; utmCSCStatus
1.3.6.1.4.1.45741.2.10.1.4.8	trapHighDiskIOUtilization	Высокая загрузка диска. Оповещение отправляется при загруженности >=95% за 5 минут хотя бы на одном из дисковых устройств	utmDiskIOUtilization
1.3.6.1.4.1.45741.2.10.1.5	utmTrafficEntities	Таблица оповещений межсетевого экрана	

OID	Наименование	Описание	Передаваемые параметры (по таблице UTM-TRAPS-BINDINGS-MIB)
1.3.6.1.4.1.45741.2.10.1.5.1	trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана	
1.3.6.1.4.1.45741.2.10.1.6	utmAccountEntities	Таблица оповещений LDAP	
1.3.6.1.4.1.45741.2.10.1.6.1	trapLDAPServerDown	Сервер LDAP недоступен	utmLDAPServerName; utmLDAPServerAddress
1.3.6.1.4.1.45741.2.10.1.7	utmThermEntities	Таблица оповещений о температуре	
1.3.6.1.4.1.45741.2.10.1.7.1	trapCriticalTemperature	Критическая температура на одном из сенсоров. Оповещение отправляется при пересечении одного из пределов рабочей температуры (нижнего или верхнего). Нижний предел рабочей температуры обычно равен 0°C (для устройств серии X -40ºC), верхний предел равен 85ºC	utmThermSensor; utmThermValue

UTM-TRAPS-BINDINGS-MIB

Файл содержит описание привязок для SNMP-уведомлений устройств UserGate и определяет объекты MIB, включаемые в сообщения о событиях и состоянии системы.

OID	Наименование	Тип данных	Описание
1.3.6.1.4.1.45741.2.11.1.1.5.1	utmSessions	integer	Текущее количество активных сессий
1.3.6.1.4.1.45741.2.11.1.1.5.2	utmSessionsMax	integer	Максимальное количество активных сессий
1.3.6.1.4.1.45741.2.11.1.1.6.1	utmUsers	integer	Количество активных пользователей на данный момент
1.3.6.1.4.1.45741.2.11.1.1.6.2	utmUsersMax	integer	Максимальное количество активных пользователей
1.3.6.1.4.1.45741.2.11.1.1.7.1	utmDataPartionFSStatus	integer	Состояние файловой системы. • 0 — clean, нормальное состояние; • 1 — not clean, требуется проверка файловой системы
1.3.6.1.4.1.45741.2.11.1.2.1.1	utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: • 0 — мастер-узел; • 1 — резервный узел; • 3 — ошибка
1.3.6.1.4.1.45741.2.11.1.2.1.2	utmHAStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • 1 — связь с узлом потеряна; • 2 — HTTP прокси-сервер недоступен; • 3 — все шлюзы недоступны; • 4 — DNS-сервер недоступен; • 5 — UserGate Management Center недоступен
1.3.6.1.4.1.45741.2.11.1.4.2.1	utmCPUUsage	integer	Загруженность центрального процессора (%)
1.3.6.1.4.1.45741.2.11.1.4.3.1	utmMemory	integer	Использование оперативной памяти (%)
1.3.6.1.4.1.45741.2.11.1.4.4.1	utmLogdiskSpace	integer	Пространство на диске, используемое под журналы (%)
1.3.6.1.4.1.45741.2.11.1.4.5.1	utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • no_raid; • 0 — optimal, массив в оптимальном состоянии; • 1 — degraded, полный или частичный выход из строя одного из дисков; • 2 — rebuild, восстановление массива
1.3.6.1.4.1.45741.2.11.1.4.5.2	utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • no_raid; • 0 — optimal, массив в оптимальном состоянии; • 1 — degraded, полный или частичный выход из строя одного из дисков. Переход в данный статус произойдет при выходе из строя 2-х дисков; • 2 — partialDegraded, полный или частичный выход из строя одного из дисков; • 3 — failed, не работает из-за наличия ошибки; • 4 — offline, диск не доступен для RAID-контроллера
1.3.6.1.4.1.45741.2.11.1.4.6.1	utmPowerSupply	integer	Количество источников питания: • 1 — один блок питания; • 2 — два блока питания
1.3.6.1.4.1.45741.2.11.1.4.6.2	utmPowerSupplyStatus	integer	Состояние источника питания: • no_power_supplies; • 0 — off, отключен; • 1 — on, включен
1.3.6.1.4.1.45741.2.11.1.4.7.1	utmCSCIfName	string	Название интерфейса
1.3.6.1.4.1.45741.2.11.1.4.7.2	utmCSCStatus	integer	Статус сетевого адаптера: • 0 — unplugged, кабель не подключен; • 1 — plugged, кабель подключен

OID	Наименование	Тип данных	Описание
1.3.6.1.4.1.45741.2.11.1.4.8.1	utmDiskIOUtilization	integer	Текущая утилизация диска (%)
1.3.6.1.4.1.45741.2.11.1.6.1.1	utmLDAPServerName	string	Название LDAP-сервера
1.3.6.1.4.1.45741.2.11.1.6.1.2	utmLDAPServerAddress	string	IP-адрес LDAP-сервера
1.3.6.1.4.1.45741.2.11.1.7.1.1	utmThermSensor	string	Название температурного сенсора
1.3.6.1.4.1.45741.2.11.1.7.1.2	utmThermValue	integer	Значение температуры, измеренное сенсором