

Table of Contents

Table of Contents	1
Диагностика и мониторинг	2
Мониторинг трафика	3
Маршруты	4
OSPF	5
VPN	6
Веб-портал	7
Заблокированные COB/L7 IP-адреса	8
Захват пакетов	9
Запросы в белый список	10
Трассировка правил	11
Ping	12
Traceroute	13
Запрос DNS	14
LLDP-соседи	15
Статистика LLDP	16
Оповещения	17
Правила оповещений	18
SNMP	19
Параметры SNMP	30
Профили безопасности SNMP	31

Documentation: 

Product: NGFW

Version: 7.x

Раздел **Мониторинг трафика** позволяет получить список всех пользовательских соединений, установленных через UserGate NGFW в реальном времени. Соединением считается уникальное сочетание адреса источника, адреса назначения и пользователя (если определен). Для каждого соединения отображаются мгновенные значения скорости передачи (TX) и скорости приема (RX). Имеется возможность сортировки выводимых данных по каждому столбцу, а также возможность создать блокирующее правило межсетевого экрана или правило ограничения пропускной способности для выбранного из списка IP-адреса источника.

Примечание Процесс построения данного отчета требует большего количества вычислительных ресурсов NGFW и при большом объеме передаваемого трафика может приводить к высокой загрузке процессора. Не рекомендуется держать данную страницу открытой во избежание излишней нагрузки на МЭ.

Маршруты

Version: 7.x

Documentation: ☒

Product: NGFW

Technology: Routing

Раздел **Маршруты** позволяет получить список всех маршрутов, указанных на определенном узле UserGate и на определенном виртуальном маршрутизаторе на узле кластера. Для просмотра маршрутов необходимо нажать на кнопку **Фильтр** и указать типы маршрутов, которые необходимо отобразить. Возможно указать следующие типы маршрутов:

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate. Данные маршруты будут помечены символом **С** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **К** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **О** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **В** в списке маршрутов.

Отображаемый список маршрутов можно скачать в виде текстового файла с помощью кнопки **Скачать все маршруты**.

OSPF

Product: NGFW

Version: 7.x

Documentation: 

Раздел **OSPF** позволяет получить отчет о состоянии канала маршрутизации. С использованием соответствующих фильтров можно отобразить информацию о протоколе на определенном узле UserGate и определенном виртуальном маршрутизаторе узла кластера. Представлена следующая информация:

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

Documentation: 

Product: NGFW

Version: 7.x

Раздел **VPN** отображает всех пользователей и все серверы, подключенные по VPN к данному серверу. Для каждого соединения отображается следующая информация:

- **Пользователь** — имя пользователя, под которым произошла аутентификация соединения.
- **Роль этого сервера** — клиент или сервер.
- **Время сессии** — продолжительность установленного соединения.
- **Туннельный IP** — адрес, назначенный данному клиенту в виртуальной частной сети.
- **IP-адрес** — адрес, с которого инициировано соединение VPN.
- **Гео IP** — страна по Geo IP, откуда установлено соединение.
- **Шифрование** — тип шифрования

Documentation: 

Product: NGFW

Version: 7.x

Раздел **Веб-портал** отображает всех пользователей и все серверы, подключенные через веб-портал к данному серверу. Для каждого соединения отображается следующая информация:

- **Имя** — имя пользователя, под которым произошла аутентификация соединения.
- **Начало сессии** — время, когда пользователь подключился к сервису.
- **Продолжительность** — продолжительность соединения.
- **IP источника** — IP-адрес пользователя.
- **Useragent** — useragent пользовательского браузера.

Можно задать период обновления данного окна от 3-х секунд до одной минуты или установить обновление вручную.

Администратор имеет возможность принудительно закрыть определённую сессию. Для этого надо выделить её и нажать кнопку **Закрыть** сессию.

Заблокированные COB/L7 IP-адреса

Documentation: 

Product: NGFW

Version: 7.x

COB отслеживает и блокирует атаки в режиме реального времени. Мерами превентивной защиты являются обрыв соединения, оповещение администратора сети и запись в журнал мониторинга.

Раздел **Заблокированные COB/L7 IP-адреса** отображает список всех заблокированных IP-адресов. Кластерные узлы имеют одну общую таблицу **Заблокированных COB/L7 IP-адресов**.

Запись в журнале отображает:

- **Заблокированный IP-адрес** — отображает заблокированный IP-адрес, возможность разблокировать и удалить IP-адрес из списка.
- **Дата блокировки** — дата и время блокировки.
- **Угроза сигнатуры** — уровень угрозы.
- **Статус журналирования** — возможность перехода в раздел журналирования:
 - для приложений trafficlog;
 - для ips сигнатуры idpslog.
- **Свойство сигнатуры/название сигнатуры** — информация о сработавшей сигнатуре.
- **IP назначения** — адрес атакованного узла.
- **Продолжительность блокировки** — время блокировки.
- **Время для снятия блокировки** — отсчет оставшегося времени, окончание блокировки.

Для разблокирования заблокированных IP-адресов необходимо выделить их в списке и нажать кнопку **Разблокировать**.

Захват пакетов

Version: 7.x

Documentation: ☒

Product: NGFW

Раздел **Захват пакетов** позволяет записать трафик, удовлетворяющий заданным условиям, в рсар-файл для дальнейшего анализа с помощью сторонних средств, например, Wireshark. Это бывает необходимо для диагностирования сетевых проблем.

Раздел состоит из трех частей:

- **Фильтры** — здесь определяются условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол Ethernet, протокол IPv4. Список протоколов IPv4 можно посмотреть [по ссылке](#).
- **Правила** — в правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.
- **Файлы** — сюда помещаются файлы с записанным трафиком. Их можно скачать для анализа или удалить.

Чтобы записать трафик, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать необходимый фильтр.	Опционально. Можно воспользоваться предустановленными фильтрами или писать весь трафик, не фильтруя его.
Шаг 2. Создать правило.	Создать правило, в котором указать имя правила, имя файла, максимальный размер записываемого файла и необходимые фильтры.
Шаг 3. Выбрать необходимое правило и начать запись.	Выбрать необходимое правило и нажать на кнопку Начать запись . По окончании прекратить запись, нажав на кнопку Остановить запись .
Шаг 4. В разделе Файлы , скачать полученный файл.	Скачать рсар-файл для анализа.

Запросы в белый список

Documentation: ☒

Product: NGFW

Version: 7.x

При блокировке сайтов с помощью правил контентной фильтрации пользователь получает страницу блокировки с указанием причины блокировки, на которой указаны имя правила, категория сайта и/или морфологическая база, черный список, из-за которых сайт был заблокирован. Кроме этого, страница блокировки предлагает пользователю сделать запрос на добавление данного сайта в белый список в случае, если пользователь не согласен с блокировкой ресурса. При нажатии на кнопку **Добавить в белый список** запрос на добавление появляется в списке запросов в разделе **Запросы в белый список**. Администратор может осуществить следующие действия с запросом пользователя:

Наименование	Описание
Добавить в белый список	Добавить данный URL в белый список. Администратору будет предложено изменить URL и выбрать белый список, в который необходимо добавить данный ресурс.
Удалить	Удалить данный запрос из списка запросов.
Отклонить URL	Добавить запрошенный URL в список отклоненных запросов. При последующих блокировках данного URL страница блокировки не будет содержать кнопки Добавить в белый список . Список отклоненных доменов и URL отображается в Окне отклоненных запросов .
Отклонить домен	Добавить домен запрошенного URL в список отклоненных запросов. При последующих блокировках любого URL данного домена страница блокировки не будет содержать кнопки Добавить в белый список . Список отклоненных доменов и URL отображается в Окне отклоненных запросов .

Администратор может проверить категорию интернет-ресурса с помощью формы **Проверить URL**. В случае, если ресурс относится к некорректной категории, администратор может сделать запрос на смену категории или изменить категорию самостоятельно локально на своем устройстве.

Для того, чтобы сделать запрос на смену категории, необходимо нажать на кнопку **Предложить категорию**. Запрос на смену категории будет отправлен в компанию UserGate, где будет проверен, и в случае подтверждения будет внесен в ближайшее обновление базы категорий сайтов UserGate URL filtering.

Для того, чтобы сменить категории локально, необходимо нажать на кнопку **Изменить категорию** и назначить до двух новых категорий. Посмотреть все сайты с измененными категориями можно в разделе **Библиотеки → Измененные категории URL**. 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**. Более подробно об изменении категорий для определенных сайтов описано в разделе руководства **Запросы в белый список**.

Трассировка правил

Documentation: ☒

Product: NGFW

Version: 7.x

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

Чтобы выполнить трассировку правил:

1. На странице **Диагностика и мониторинг** в разделе **Трассировка правил** нажмите **Настроить** и укажите параметры фильтра 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.

Примечание Если фильтр не настроен, то могут быть также отображены результаты обработки запросов других пользователей.

2. Сохраните изменения.

3. Нажмите **Начать**.

4. Попросите пользователя открыть проблемный сайт и посмотрите, какие правила срабатывают при открытии сайта. Будут указаны все правила, которые выполняются во время обработки пользовательского запроса.

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

Администратор может проверить содержание отображаемого в трассировке интернет-ресурса с помощью формы **Открыть сайт**. С помощью формы **Добавить в белый список** администратор может поместить выбранный ресурс в один из существующих в системе списков URL.

Ping

Documentation: ☒
Product: NGFW
Version: 7.x

С помощью утилиты ping можно диагностировать доступность сетевых ресурсов. Параметры команды ping:

Наименование	Описание
Ping host	Хост, который необходимо проверить.
TTL	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту.
Интерфейс	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации.
Счетчик	Количество повторов.
Показывать timestamp	Добавляет timestamp в вывод команды.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Traceroute

Product: NGFW

Documentation: ☒

Version: 7.x

С помощью утилиты traceroute можно проверить путь следования сетевых пакетов к определенному хосту. Параметры команды traceroute:

Наименование	Описание
Traceroute host	Хост, который необходимо проверить.
Использовать ICMP	Использовать протокол ICMP для выполнения команды traceroute. Если не указано, то используется протокол UDP.
Интерфейс	С какого сетевого интерфейса выполнять команду.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Запрос DNS

Documentation: ☒
Product: NGFW
Version: 7.x

Используя запрос DNS, администратор может проверить работу DNS-серверов.

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	DNS сервер, куда посылать запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

LLDP-соседи

Documentation: ☒
Product: NGFW
Version: 7.x

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](#)».

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

Параметр	Описание
Chassis ID	Идентификатор шасси; является обязательной TLV-записью LLDP-кадра. 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-адреса интерфейса управления (IPv4 и IPv6). • Номер интерфейса 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); является обязательной TLV-записью LLDP-кадра. В качестве идентификатора используется MAC-адрес интерфейса
PortDescr	Описание порта
TTL	Время жизни передаваемых пакетов LLDP; является обязательной TLV-записью LLDP-кадра. TTL задаётся в разделе UserGate → Настройки → Модули в поле Настройка LLDP

Documentation: ☒
Product: NGFW
Version: 7.x

Данная вкладка отображает статистику интерфейсов, в настройках которых был указан профиль LLDP. Отображается следующая информация:

Наименование	Описание
Interface	Название интерфейса.
Transmitted	Общее количество кадров LLDP, переданных через интерфейс.
Received	Общее количество кадров LLDP, полученных на интерфейс.
Discarded	Число полученных на этом интерфейсе кадров LLDP, которые были отброшены.
Unrecognized	Количество кадров LLDP с неподтверждённым содержимым, полученных на этом интерфейсе.
Ageout	В каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется.
Inserted	Количество добавлений записей с информацией о соседях LLDP.
Deleted	Количество удалений записей о соседях LLDP.

Оповещения

Правила оповещений

Documentation: ☒
Product: NGFW
Version: 7.x

Данный раздел позволяет определить правила оповещений, которые в дальнейшем можно использовать для отсылки оповещений о различных типах событий, например, высокой загрузке CPU или отправке пароля пользователю по SMS. Для создания правила оповещений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать один или несколько профилей оповещения.	Смотрите раздел Профили оповещений .
Шаг 2. Создать группы получателей оповещений.	Смотрите разделы Почтовые адреса и Номера телефонов .
Шаг 3. Создать правило оповещения.	Во вкладке Диагностика и мониторинг в разделе Оповещения → Правила оповещений добавить правило.

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.
Профиль оповещения	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде email-адресов.
От	От кого будет приходить оповещение.
Тема	Тема оповещения.
Таймаут перед повторной отправкой, секунд	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
События	Укажите события, для которых необходимо получать оповещения.
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения.

Documentation: ☒
Product: NGFW
Version: 7.x

UserGate NGFW поддерживает мониторинг по протоколам SNMP v2c и SNMP v3. Реализована поддержка как SNMP-запросов (SNMP queries), так и уведомлений (SNMP traps), что позволяет контролировать критически важные параметры устройства с помощью корпоративных платформ SNMP-мониторинга.

Для настройки мониторинга с помощью SNMP:

1. Откройте доступ к сервису SNMP в свойствах зоны интерфейса, к которому будет происходить подключение по протоколу SNMP.
2. Создайте правило SNMP.

Для создания правила SNMP перейдите в раздел **Диагностика и мониторинг → Оповещения → SNMP**, нажмите **Добавить** и укажите значения параметров правила.

Параметр	Описание
Название правила	Название правила
IP-адрес сервера для трапов	IP-адрес сервера для уведомлений и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Параметр необходим только в случае, если необходимо отправлять уведомления (SNMP traps) на сервер оповещений
Комьюнити	SNMP community — строка для идентификации UserGate NGFW и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и 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 разрешает получение и обработку SNMP-запросов от SNMP-менеджера
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-уведомлений на сервер, настроенный для приема оповещений
Название профиля безопасности SNMP	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP
События	Выбор типов параметров, доступных для мониторинга по правилу

ПримечаниеПараметры аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования — в профиле безопасности SNMP) на SNMP-менеджере должны совпадать с соответствующими параметрами SNMP на устройстве.

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

Компании UserGate присвоен уникальный идентификатор SNMP PEN (Private Enterprise Number) — 45741.

Актуальные mib-файлы устройства UserGate с параметрами мониторинга можно скачать из консоли администратора устройства. Для этого перейдите на вкладку **Диагностика и мониторинг**, далее в разделе **Оповещения → SNMP** нажмите **Скачать MIB**.

Для скачивания доступны следующие MIB-файлы:

- UTM-TRAPS-MIB.

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

UTM-TRAPS-MIB

Параметр	Описание
trapCoreCrush	Сбой ядра
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен
trapCoreBootstrapEnd	Загрузка сервера завершена успешно
trapDefaultGatewayChanged	Изменение шлюза по умолчанию
trapHighSessionsCounter	Таблица сессий заполнена на 90%
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии
trapDataPartitionFSStatus	Статус файловой системы. Состояние файловой системы изменилось на not_clean
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен»
trapMemberDown	Узел отказоустойчивого кластера отключен
trapAttackDetected	Обнаружение атаки системой COB
trapChecksumFailed	Нарушение целостности бинарных файлов
trapHighCPUUsage	Высокая загрузка центрального процессора (95%)
trapLowMemory	Высокая загрузка памяти (95%)
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов
trapRaidStatus	Изменение статуса RAID
trapPowerSupply	Первый источник питания отключен
trapCableStatus	Кабель был подключен или отключен от интерфейса
trapHighDiskIOUtilization	Высокая загрузка диска. Оповещение отправляется при загрузке >=95% за 5 минут хотя бы на одном из дисковых устройств
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана
trapLDAPServerDown	Сервер LDAP недоступен

Параметр	Описание
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 -40°C), верхний предел равен 85°C

UTM-TRAPS-BINDINGS-MIB

Параметр	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий
utmSessionsMax	integer	Максимальное количество активных сессий
utmUsers	integer	Количество активных пользователей на данный момент
utmUsersMax	integer	Максимальное количество активных пользователей
utmDataPartionFSStatus	integer	Состояние файловой системы. 0 — clean, нормальное состояние; 1 — not clean, требуется проверка файловой системы
utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: 0 — мастер-узел; 1 — резервный узел; 3 — ошибка
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
utmCPUUsage	integer	Загруженность центрального процессора (%)
utmMemory	integer	Использование оперативной памяти (%)
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы (%)
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

Параметр	Тип данных	Описание
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
utmPowerSupply	integer	Количество источников питания: 1 — один блок питания; 2 — два блока питания
utmPowerSupplyStatus	integer	Состояние источника питания: - no_power_supplies; 0 — off, отключен; 1 — on, включен
utmCSCIfName	string	Название интерфейса
utmCSCStatus	integer	Статус сетевого адаптера: 0 — кабель не подключен; 1 — кабель подключен
utmDiskIOUtilization	integer	Текущая утилизация диска (%)
utmLDAPServerName	string	Название LDAP-сервера
utmLDAPServerAddress	string	IP-адрес LDAP-сервера
utmThermSensor	string	Название температурного сенсора
utmThermValue	integer	Значение температуры, измеренное сенсором

UTM-MIB

Параметр	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается фактическое число загруженных виртуальных процессоров
usersCounter	integer	Количество активных пользователей на текущий момент времени. (*)
sessionsCounter	integer	Количество активных сессий на текущий момент времени. (*)

Параметр	Тип данных	Описание
tcpSessionsCounter	integer	Количество активных TCP-сессий на текущий момент времени. (*)
udpSessionsCounter	integer	Количество активных UDP-сессий на текущий момент времени. (*)
icmpSessionsCounter	integer	Количество активных ICMP-сессий на текущий момент времени. (*)
sessionsRate10	integer	Количество новых сессий в секунду. Среднее значение за последние 10 секунд. (*)
sessionsRate60	integer	Количество новых сессий в секунду. Среднее значение за последние 60 секунд. (*)
sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд. (*)
tcpSessionsRate10	integer	Количество новых TCP-сессий в секунду. Среднее значение за последние 10 секунд. (*)
tcpSessionsRate60	integer	Количество новых TCP-сессий в секунду. Среднее значение за последние 60 секунд. (*)
tcpSessionsRate300	integer	Количество новых TCP-сессий в секунду. Среднее значение за последние 300 секунд. (*)
udpSessionsRate10	integer	Количество новых UDP-сессий в секунду. Среднее значение за последние 10 секунд. (*)
udpSessionsRate60	integer	Количество новых UDP-сессий в секунду. Среднее значение за последние 60 секунд. (*)
udpSessionsRate300	integer	Количество новых UDP-сессий в секунду. Среднее значение за последние 300 секунд. (*)
icmpSessionsRate10	integer	Количество новых ICMP-сессий в секунду. Среднее значение за последние 10 секунд. (*)
icmpSessionsRate60	integer	Количество новых ICMP-сессий в секунду. Среднее значение за последние 60 секунд. (*)
icmpSessionsRate300	integer	Количество новых ICMP-сессий в секунду. Среднее значение за последние 300 секунд. (*)
dnsRequestCounter	integer	Общее количество DNS-запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS-запросов. (*)
dnsRequestRate	integer	Количество DNS-запросов в секунду. (*)
httpRequestCounter	integer	Общее количество HTTP-запросов. (*)
httpBlockedRequestCounter	integer	Количество заблокированных HTTP-запросов. (*)
httpRequestRate	integer	Количество HTTP-запросов в секунду. (*)
dataPartitionFSStatus	string	Состояние файловой системы: • clean — нормальное состояние; • not_clean — требуется проверка файловой системы

Параметр	Тип данных	Описание
haStatus	integer	Текущий статус узла кластера отказоустойчивости: 0 — мастер-узел; 1 — резервный узел; 3 — ошибка
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %.
memoryUsed	integer	Использование оперативной памяти; отображается в %.
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.
powerSupply1Status	string	Состояние первого источника питания: - no_power_supplies; - on — включен; - off — отключен
powerSupply2Status	string	Состояние второго источника питания: - no_power_supplies; - on — включен; - off — отключен
raidType	string	Тип RAID массива
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
diskIOUtilization	integer	Текущая утилизация диска (%)
diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд
diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд

ПримечаниеМетрики, отмеченные в описании символом (*) не актуальны для UGMC и LogAn. Значения метрик для этих устройств будут всегда равны нулю.

UTM-INTERFACES-MIB

Параметр	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber
ifDescr	string	Информация об интерфейсе, которая может включать в себя название производителя, имя продукта, аппаратную версию интерфейса

Параметр	Тип данных	Описание

Параметр	Тип данных	Описание
ifType	integer	Тип интерфейса, определенный в соответствии с протоколом физического/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, используемый 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, используемый 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
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс

Параметр	Тип данных	Описание
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду. Максимальное значение: 4 294 967 295 ($\approx 4,29$ Гбит/с). Рекомендуется использовать для интерфейсов со скоростью до 4,29 Гбит/с, когда требуется высокая точность
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес)
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
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, сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов нижнего уровня не работает
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки
ifInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены

Параметр	Тип данных	Описание
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передачи. Одна из возможных причин отбрасывания: освобождение буферного пространства
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок
ifOutQLen	gauge32	Длина выходной очереди (в пакетах)
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены
ifHCInOctets	counter64	Параметр, аналогичный ifInOctets — количество байтов, принятое данным интерфейсом, включая служебные; используется счетчик большей емкости
ifHCInUcastPkts	counter64	Параметр, аналогичный ifInUcastPkts — количество доставленных пакетов одноадресной рассылки; используется счетчик большей емкости
ifHCInMulticastPkts	counter64	Параметр, аналогичный ifInMulticastPkts — количество доставленных пакетов многоадресной рассылки; используется счетчик большей емкости
ifHCInBroadcastPkts	counter64	Параметр, аналогичный ifInBroadcastPkts — количество доставленных широковещательных пакетов; используется счетчик большей емкости
ifHCOctets	counter64	Параметр, аналогичный ifOutOctets — количество байтов, переданное данным интерфейсом, включая служебные; используется счетчик большей емкости
ifHCOUcastPkts	counter64	Параметр, аналогичный ifOutUcastPkts — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
ifHCOmulticastPkts	counter64	Параметр, аналогичный ifOutMulticastPkts — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
ifHCOBroadcastPkts	counter64	Параметр, аналогичный ifOutBroadcastPkts — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • 1 — enabled, включено; • 2 — disabled, отключено
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

Параметр	Тип данных	Описание
ifPromiscuousMode	integer	«Неразборчивый режим». Возможные значения: 1 — true, станция принимает все пакеты/кадры независимо от того, кому они адресованы; 2 — false, интерфейс принимает только пакеты/кадры, адресованные этой станции; Значение объекта не влияет на прием широковещательных и многоадресных пакетов/кадров
ifAlias	string	Название интерфейса, заданное администратором при настройке интерфейса
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счетчиков интерфейса
ifName	string	Текстовое имя интерфейса, используемое в системе (например, port0)
ipAdEntAddr	IpAddress	IP-адрес интерфейса
ipAdEntIfIndex	integer	Индекс интерфейса, к которому привязан данный IP-адрес

UTM-TEMPERATURE-MIB

Параметр	Тип данных	Описание
thermNumber	integer	Количество температурных сенсоров на данной платформе
thermLowerThreshold	integer	Нижний предел рабочей температуры
thermUpperThreshold	integer	Верхний предел рабочей температуры
thermTable	sequence	Таблица температурных сенсоров с показаниями (thermEntry)
thermEntry	sequence	Информация о конкретном сенсоре: - thermName (string) — название сенсора; - thermValue (integer) — показание сенсора; - thermUnit (string) — единица измерения показаний сенсора

Примечание Данные температурных сенсоров будут отображаться только для поддерживаемых аппаратных платформ. В настоящий момент поддерживаются устройства UserGate C150, C151, FG, X10. Для неподдерживаемых платформ или виртуальных решений таблица сенсоров будет пустой, а значения количества сенсоров и пределы рабочих температур будут равны нулю.

Примечание Если с сенсора не удалось снять показание температуры, он не будет передан в таблице, при этом параметр thermNumber подсчитывает общее количество температурных сенсоров, даже с учетом неработающих. В таком случае количество сенсоров в таблице и значение thermNumber могут не совпадать.

Параметры SNMP

Documentation: ☒
Product: NGFW
Version: 7.x

Данный раздел используется для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP. Параметры SNMP задаются для каждого узла индивидуально.

Наименование	Описание
SNMP имя системы	Название системы, используемое подсистемой управления SNMP.
SNMP локация системы	Информация о физическом расположении SNMP-агента.
SNMP описание системы	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину, тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа text. Engine ID может быть сформирован в формате: - IPv4 (ip4). - IPv6 (ipv6). - MAC-адрес (mac). - Текст (text). - Октеты (octets).

Профили безопасности SNMP

Documentation: ☒
Product: NGFW
Version: 7.x

В данном разделе производится настройка профилей безопасности для аутентификации SNMPv3-менеджера.

Примечание Настройки аутентификации для SNMP v3 (имя пользователя, пароль, тип и алгоритм аутентификации, алгоритм и пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate

Наименование	Описание
Название	Название профиля безопасности SNMP
Описание	Описание профиля безопасности SNMP
Пользователь	Имя пользователя для аутентификации SNMP-менеджера.
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации. Возможно использовать: • SHA1; • MD5; • SHA224; • SHA256; • SHA384; • SHA512.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.

