

Table of Contents

Table of Contents	1
Настройка устройства	2
Общие настройки	3
Управление устройством	7
Кластеризация и отказоустойчивость	10
Управление доступом к консоли NGFW	16
Управление сертификатами	19
Интерфейс командной строки (CLI)	23
Системные утилиты	28

Общие настройки

Documentation: ☒

Version: 6.1.9, 7.0.1

Product: UserGate NGFW

Раздел **Общие настройки** определяет базовые установки NGFW:

Наименование	Описание
Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п.
Язык интерфейса по умолчанию	Язык, который будет использоваться по умолчанию в консоли.
Режим авторизации веб-консоли	Способ аутентификации пользователя (администратора) при входе в веб-консоль управления. Возможны следующие варианты: • По имени и паролю. Администратор должен ввести имя и пароль для получения доступа к веб-консоли. • По X.509-сертификату. Для авторизации по сертификату необходимо иметь сертификат пользователя, подписанный сертификатом удостоверяющего центра веб-консоли и установленный в браузер. При включении этого режима авторизации режим авторизации по имени и паролю отключается. Вернуть режим авторизации по имени и паролю можно с помощью команд CLI.
Профиль SSL для веб-консоли	Выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробно о профилях SSL смотрите в главе Профили SSL .
Профиль SSL для страниц блокировки/авторизации	Выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации Captive-портала. Подробно о профилях SSL смотрите в главе Профили SSL .
Настройка времени сервера	Настройка параметров установки точного времени. • Использовать NTP — использовать сервера NTP из указанного списка для синхронизации времени. • Основной сервер NTP — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org. • Запасной сервер NTP — адрес запасного сервера точного времени. • Время на сервере — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.

Наименование	Описание
Модули	Позволяет настроить модули UserGate: • HTTP(S)-прокси порт — позволяет указать нестандартный (дополнительный) номер порта, который будет использоваться для подключения к встроенному прокси-серверу. По умолчанию используется порт TCP 8090; при изменении порт продолжает функционировать. Важно! Нельзя использовать следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100. • Домен auth captive-портала — служебный домен, который используется UserGate при авторизации пользователей через Captive-портал. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя auth.captive, которое может быть изменено на другое доменное имя, принятое в организации. • Домен logout captive-портала — служебный домен, который используется пользователями UserGate для окончания сессии (logout). Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя logout.captive, которое может быть изменено на другое доменное имя, принятое в организации. • Домен страницы блокировки — служебный домен, который используется для отображения страницы блокировки пользователям. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то резолвинг настроен автоматически. По умолчанию используется имя block.captive, которое может быть изменено на другое доменное имя, принятое в организации. • FTP поверх HTTP — включение или отключение модуля, позволяющего получать доступ к содержимому FTP-серверов из пользовательского браузера. Требуется явное указание прокси-сервера для протокола FTP в браузере пользователя. Администратор может ограничивать доступ к ресурсам FTP с помощью правил контентной фильтрации (только по условиям Пользователи и URL). • FTP поверх HTTP домен — служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то резолвинг настроен автоматически. По умолчанию используется имя ftpclient.captive, которое может быть изменено на другое доменное имя, принятое в организации. • SNMP 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 (ip6). • MAC-адрес (mac). • Текст (text). • Октеты (octets). • Пароль агентов терминального сервиса — настройка пароля для подключения агентов авторизации терминальных серверов.

Наименование	Описание
Настройка кэширования HTTP	Настройка кэша прокси-сервера: • Включен/Выключен — включение или отключение кэширования. • Исключения кэширования — список URL, которые не будут кэшироваться. • Максимальный размер объекта, Мбайт — объекты с размером более, чем указано в данной настройке, не будут кэшироваться. Рекомендуется оставить значение по умолчанию — 1 Мбайт. • Размер RAM-кэша, Мбайт — размер оперативной памяти, отведенный под кэширование. Не рекомендуется ставить более 20% от объема оперативной памяти системы. Внимание! Данный функционал нужен только при очень медленном интернет соединении. В обычных условиях его включение приводит к задержкам и лишнему использованию ресурсов.
Log Analyzer	Настройки модуля LogAn: • Локальный сервер/Внешний сервер. Выберите внешний сервер, если у вас есть внешний сервер Log Analyzer, в противном случае выберите локальный сервер. • Состояние — показывает текущее состояние сервиса статистики. Важно! При указании внешнего LogAn обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером LogAn.
Web-портал	Настройки для предоставления доступа к внутренним ресурсам компании с помощью веб-портала (SSL VPN). Подробное описание данных настроек смотрите в главе Веб-портал.
Настройка PCAP	Настройка записи трафика при срабатывании сигнатур системы обнаружения вторжений. Настройка захвата пакетов: • Без захвата. • Один пакет. • Предшествующие пакеты (от 4 до 30 пакетов). • Предшествующие и последующие пакеты (предшествующие: от 4 до 30; последующие: от 2 до 15). Важно! Большой размер PCAP может вести к значительному замедлению обработки данных.
Настройка учета изменений	При включении данной опции и создания Типов изменений любое изменение в конфигурацию, вносимое администратором через веб-консоль, будет требовать указание типа изменения и описания вносимого изменения. В качестве типов изменения могут быть, например, указаны: • Распоряжение. • Приказ. • Регламентные работы, и т.д. Количество типов изменений не ограничено.
Агент UserGate Management Center	Настройки для подключения устройства к центральной консоли управления, позволяющей управлять парком устройств UserGate из одной точки; для подключения к UGMC используются порты TCP 2022 и TCP 9712. • Включен/Выключен — включение или отключение управления с помощью UGMC. • Адрес UserGate Management Center — адрес UGMC. • Код устройства — токен, требуемый для подключения к UGMC. UGMC может использоваться как источник обновления ПО и сигнатур.

Наименование	Описание
Расписание скачивания обновлений	Настройки для управления скачиванием обновлений программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке (база категорий URL-фильтрации, COB, списки IP-адресов, URL, типов контента и другие). • Обновления ПО — настройка расписания проверки наличия новых обновлений UGOS и скачивания обновлений. • Обновления библиотек — настройка расписания проверки наличия новых обновлений библиотек и скачивания библиотек. Чекбокс Единое расписание для всех обновлений применяет расписание ко всем библиотекам, иначе для каждой библиотеки необходимо настроить собственное расписание. При задании расписания возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".

Раздел **Управление устройством** определяет следующие настройки UserGate:

- Кластеризация.
- Настройки диагностики.
- Операции с сервером.
- Экспорт и импорт настроек.

Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки UserGate при решении возможных проблем.

Наименование	Описание
Детализация диагностики	• Off - ведение журналов диагностики отключено. • Error - журналировать только ошибки работы сервера. • Warning - журналировать только ошибки и предупреждения. • Info - журналировать только ошибки, предупреждения и дополнительную информацию. • Debug - максимум детализации. Рекомендуется установить значение параметра Детализация диагностики в Error (только ошибки) или Off (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность UserGate.
Журналы диагностики	• Скачать журналы - скачать диагностические журналы для передачи их в службу поддержки UserGate; для скачивания доступны журналы веб-консоли и/или журналы системы. Для скачивания необходимо выбрать журналы и нажать Начать архивирование журналов; после архивирования журналы будут доступны для скачивания (кнопка Скачать). • Очистить журналы - очистить содержимое журналов.
Удаленный помощник	• Включено/Отключено - включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UserGate для диагностики и решения проблем. Для успешной активации удаленного помощника UserGate должен иметь доступ к серверу удаленного помощника по протоколу SSH. • Идентификатор удаленного помощника - полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • Токен удаленного помощника - полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• Перезагрузить - перезагрузка сервера UserGate. • Выключить - выключение сервера UserGate.
Обновления	Выбор канала обновлений ПО UserGate • Стабильные - проверка наличия стабильных обновлений ПО. • Бета - проверка наличия экспериментальных обновлений.

Команда UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UserGate в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе [Лицензирование UserGate](#)). При наличии обновлений в разделе **Управление устройством** → **Операции с сервером** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом

возможного времени простоя UserGate.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния UserGate, как это описано в разделе Системные утилиты . Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления	В разделе Управление устройством при наличии оповещения Доступны новые обновления нажать на ссылку Установить сейчас . Система установит скачанные обновления, по окончании установки UserGate будет перезагружен.

Экспорт и импорт настроек

Администратор имеет возможность сохранить текущие настройки UserGate в файл и впоследствии восстановить эти настройки на этом же или другом сервере UserGate. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

ПримечаниеЭкспорт настроек является кластерной функцией, т.е. экспортируется конфигурация всех узлов кластера. При импорте конфигурации будет предложен выбор нужного узла кластера для восстановления.
ПримечаниеЭкспорт/импорт настроек не восстанавливает состояние кластера и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать UserGate с помощью имеющегося ПИН-кода и заново создать кластер, если это необходимо.
ПримечаниеВ случае использования мультифакторной аутентификации через TOTP, ключи TOTP не сохраняются; необходима повторная инициализация.

Имеется возможность сделать экспорт всех настроек (за исключением вышеперечисленных), либо сделать только экспорт сетевых настроек. При экспорте только сетевых настроек сохраняется информация о:

- Настройки DNS.
- Настройки DHCP.
- Настройки всех интерфейсов, включая туннели.
- Настройки шлюзов.
- Настройки виртуальных маршрутизаторов (VRF).
- Настройки WCCP.
- Настройки зон.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе Управление устройством нажать на ссылку Экспорт и импорт настроек → Экспорт → Экспортировать все настройки или Экспортировать сетевые настройки . Система сохранит текущие настройки сервера под именем utm-utmcore@nodename_version-YYYYMMDD_HHMMSS.bin, где nodename - имя узла UserGate version - версия UGOS YYYYMMDD_HHMMSS - время выгрузки настроек в часовом поясе UTC, например: utm-utmcore@heashostatot_6.1.1.10462R-1_20210511_095942

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе Управление устройством → Экспорт и импорт настроек нажать Импорт и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен.

ПримечаниеДля корректного импорта правил, использующих обновляемые списки UserGate (приложения, категории URL и т.п.), необходимо наличие лицензии на модули SU и ATP, а также загруженных списков UserGate.

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе Управление устройством → Экспорт и импорт настроек нажать кнопку Добавить , указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила Удаленный сервер указать параметры удаленного сервера: • Тип сервера - FTP или SSH. • Адрес сервера - IP-адрес сервера. • Порт - порт сервера. • Логин - учетная запись на удаленном сервере. • Пароль/Подтверждение пароля - пароль учетной записи. • Путь на сервере - путь на сервере, куда будут выгружены настройки.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила Расписание указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) - обозначает весь диапазон (от первого до последнего). • Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Technology: Clustering and HA
Version: 6.1.9, 7.0.1
Product: NGFW
Documentation: ☒

NGFW поддерживает 2 типа кластеров:

- 1. **Кластер конфигурации.** Узлы, объединенные в кластер конфигурации, поддерживают единые настройки в рамках кластера.
 - 2. **Кластер отказоустойчивости.** До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив. Возможно собрать несколько кластеров отказоустойчивости.
- Важно**В кластере поддерживается работа разных версий виртуального исполнения и моделей аппаратных устройств UserGate, а так же смешанные кластера для аппаратных и виртуальных исполнений.

Кластер конфигурации

Ряд настроек уникален для каждого из узлов кластера, например, настройка сетевых интерфейсов и IP-адресация. Список уникальных настроек:

Наименование	Описание
Настройки, уникальные для каждого узла	Настройки Log Analyzer. Настройки диагностики. Настройки интерфейсов. Настройки шлюзов. Настройки DHCP. Маршруты. Настройки OSPF. Настройки BGP.

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выполнить первоначальную настройку на первом узле кластера.	Смотрите главу Первоначальная настройка .
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера.	В разделе Зоны создать выделенную зону для репликации настроек кластера или использовать существующую (Cluster). В настройках зоны разрешить следующие сервисы: - Консоль администрирования - Кластер Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.
Шаг 3. Указать IP-адрес, который будет использоваться для связи с другими узлами кластера.	В разделе Управление устройством в окне Кластер конфигурации выбрать текущий узел кластера и нажать на кнопку Редактировать . Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
Шаг 4. Сгенерировать Секретный код на первом узле кластера.	В разделе Управление устройством нажать на кнопку Сгенерировать секретный код . Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.

Наименование	Описание
Шаг 5. Подключить второй узел в кластер.	Подключиться к веб-консоли второго узла кластера, выбрать язык установки. Указать интерфейс, который будет использован для подключения к первому узлу кластера и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети, например, интерфейсам eth2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку Подключить. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и все настройки первого кластера реплицируются на второй. Состояние узлов кластера конфигурации можно определить по цветовой индикации напротив названия узла UserGate в разделе UserGate → Управление устройством → Кластер конфигурации : • Зелёный: узел доступен. • Жёлтый: происходит синхронизация между узлами кластера конфигурации. • Красный: связь до узла потеряна, узел недоступен.
Шаг 6. Назначить зоны интерфейсам второго узла.	В веб-консоли второго узла кластера в разделе Сеть → Интерфейсы необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера.
Шаг 7. Настроить параметры, индивидуальные для каждого узла кластера (опционально).	Настроить шлюзы, маршруты, параметры OSPF, BGP, индивидуальные для каждого из узлов.

До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самых кластеров отказоустойчивости может быть несколько, например, в кластер конфигурации добавлены узлы A, B, C и D на основе которых создано 2 кластера отказоустойчивости - A-B и C-D.

Поддерживаются 2 режима кластера отказоустойчивости - **Актив-Актив** и **Актив-Пассив**. Состояние узлов кластера можно определить по цвету индикатора около названия узла UserGate в разделе **UserGate → Управление устройством → Кластеры отказоустойчивости** :

- **Красный**: нет связи с соседними узлами конфигурации.
- **Жёлтый**: кластер отказоустойчивости не запущен на узле.

Отсутствие индикатора напротив названия узла говорит о доступности узла кластера.

Кластер отказоустойчивости Актив-Пассив

В режиме Актив-Пассив один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных. На каждом из узлов кластера выбираются сетевые интерфейсы, которым администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии.

Примечание Режим Актив-Пассив поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другой, за исключением сессий, использующих прокси сервер, например, трафик HTTP/S.

При переходе роли мастер на резервный сервер на него переносятся **все** виртуальные IP-адреса **всех** кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети (Таймеры: Adver - 1сек, MasterDown - 3сек), например, если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (смотрите раздел [Настройка шлюзов](#)), и доступ в интернет отсутствует через все имеющиеся шлюзы.

Если хост, указанный в свойствах проверки сети, недоступен на всех узлах кластера, то кластер отказоустойчивости будет отключен.

- Сбой в работе ПО NGFW.

Отключение одного или нескольких сетевых интерфейсов, на которых назначены виртуальные IP-адреса понижает приоритет узла, но не обязательно приведет к изменению роли сервера. Переход на запасной узел произойдет, если приоритет запасного узла окажется выше, чем мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла равен 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, у которого отсутствует физическое подключение к сети. Соответственно, для кластера отказоустойчивости, состоящего из двух узлов, при пропадании физического подключения к сети одного интерфейса на мастер-узле, роль мастера переместится на запасной сервер, если на запасном сервере все кластерные интерфейсы подключены к сети (приоритет мастер-сервера будет равен 248, приоритет резервного - 249). При восстановлении физического подключения на первоначальном мастер-узле роль мастера вернется обратно на него, поскольку его приоритет вернется в значение 250 (справедливо для случая если виртуальные адреса сконфигурированы на двух и более интерфейсах. Если на одном, то роль мастера не возвращается).

Отключение одного или нескольких кластерных сетевых интерфейсов **на запасном узле**, понижает приоритет узла, тем не менее данный запасной узел может стать мастер-узлом при безусловном переходе роли, или в случае, когда приоритет мастер узла станет меньше, чем приоритет данного запасного узла.

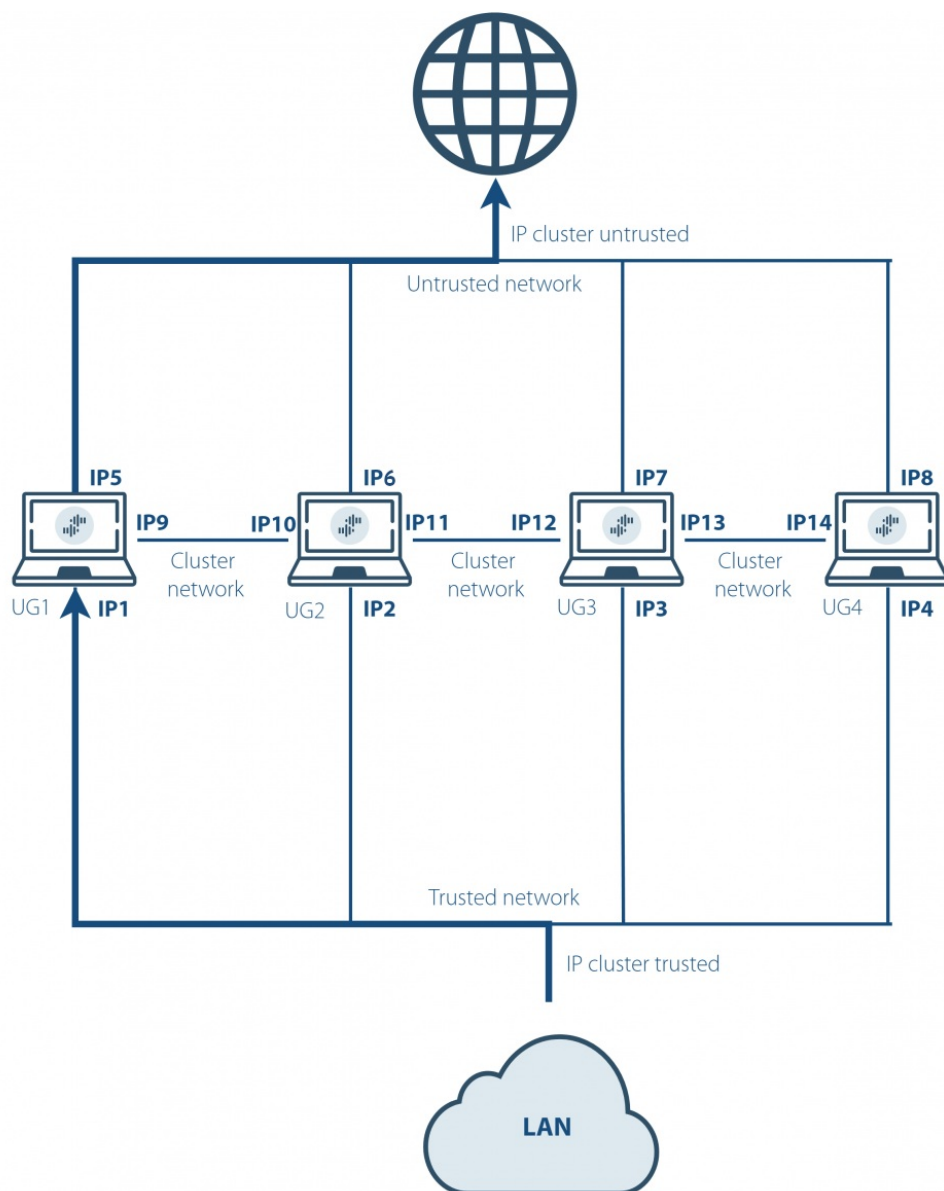
Примечание Если кластерные IP-адреса назначены VLAN-интерфейсам, то отсутствие подключения на физическом интерфейсе будет трактоваться кластером отказоустойчивости как потеря соединения на всех VLAN-интерфейсах, созданных на данном физическом интерфейсе.

Примечание Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на запасной узел при переключении, NGFW посылают служебное оповещение GARP (Gratuitous ARP), извещающий сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. Пакет GARP отсылается NGFW каждую минуту и при переезде роли мастера на запасной узел.

Ниже представлена пример сетевой диаграммы отказоустойчивого кластера в режиме Актив-Пассив. Интерфейсы настроены следующим образом:

- **Зона Trusted:** IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Untrusted:** IP5, IP6, IP7, IP8 и IP cluster (Untrusted).
- **Зона Cluster:** IP9, IP10, IP11, IP12, IP13, IP14. Интерфейсы в зоне Cluster используются для репликации настроек.

Оба кластерных IP-адреса находятся на узле UG1. Если узел UG1 становится недоступным, то оба кластерных IP-адреса перейдут на следующий узел, который станет мастер узлом, например, UG2.



Отказоустойчивый кластер в режиме Актив-Пассив

Кластер отказоустойчивости Актив-Актив

В режиме Актив-Актив один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера. На каждом из узлов кластера выбираются сетевые интерфейсы, которым администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии.

Виртуальные IP-адреса всегда находятся на интерфейсах Мастер-узла, поэтому Мастер-узел получает ARP-запросы клиентов и отвечает на них, последовательно отдавая MAC-адреса всех узлов отказоустойчивого кластера, обеспечивая равномерное распределение трафика на все узлы кластера, учитывая при этом необходимость неразрывности пользовательских сессий.

ПримечаниеБалансировка трафика будет работать только в одном широковебательном домене. Для примера, если для клиентов VIP-адрес будет шлюзом по умолчанию, то балансировка трафика будет работать, так как разным клиентам будут поочередно отдаваться разные MAC-адреса узлов, но в случае, если между NGFW и клиентами находится маршрутизатор, то балансировка работать не будет, так как ARP-запрос на VIP-адрес пошлет только сам маршрутизатор и ему вернется MAC-адрес только одного из узлов, через который он и отправит весь трафик.

ПримечаниеРежим Актив-Актив поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другой, за исключением сессий, использующих прокси сервер, например, трафик HTTP/S.

При переходе роли мастер на резервный сервер на него переносятся **все** виртуальные IP-адреса **всех** кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети(Таймеры: Adver - 1сек, MasterDown - 3сек), например, если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (смотрите раздел [Настройка шлюзов](#)), и доступ в интернет отсутствует через все имеющиеся шлюзы.
- Сбой в работе ПО NGFW.

Отключение одного или нескольких сетевых интерфейсов **мастер-узла**, на которых назначены виртуальные IP-адреса, понижает приоритет узла, но не обязательно приведет к изменению роли сервера. Переход на запасной узел произойдет, если приоритет запасного узла окажется выше, чем мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла равен 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, у которого отсутствует физическое подключение к сети. Соответственно, для кластера отказоустойчивости, состоящего из двух узлов, при пропадании физического подключения к сети одного интерфейса на мастер-узле, роль мастера переместится на запасной сервер, если на запасном сервере все кластерные интерфейсы подключены к сети (приоритет мастер-сервера будет равен 248, приоритет резервного - 249). При восстановлении физического подключения на первоначальном мастер-узле роль мастера вернется обратно на него, поскольку его приоритет вернется в значение 250.

Отключение одного или нескольких кластерных сетевых интерфейсов **на запасном узле**, понижает приоритет узла, а также исключает данный узел из балансировки трафика. Тем не менее данный запасной узел может стать мастер-узлом при безусловном переходе роли, или в случае, когда приоритет мастер узла станет меньше, чем приоритет данного запасного узла.

ПримечаниеЕсли кластерные IP-адреса назначены VLAN-интерфейсам, то отсутствие подключения на физическом интерфейсе будет трактоваться кластером отказоустойчивости как потеря соединения на всех VLAN-интерфейсах, созданных на данном физическом интерфейсе.

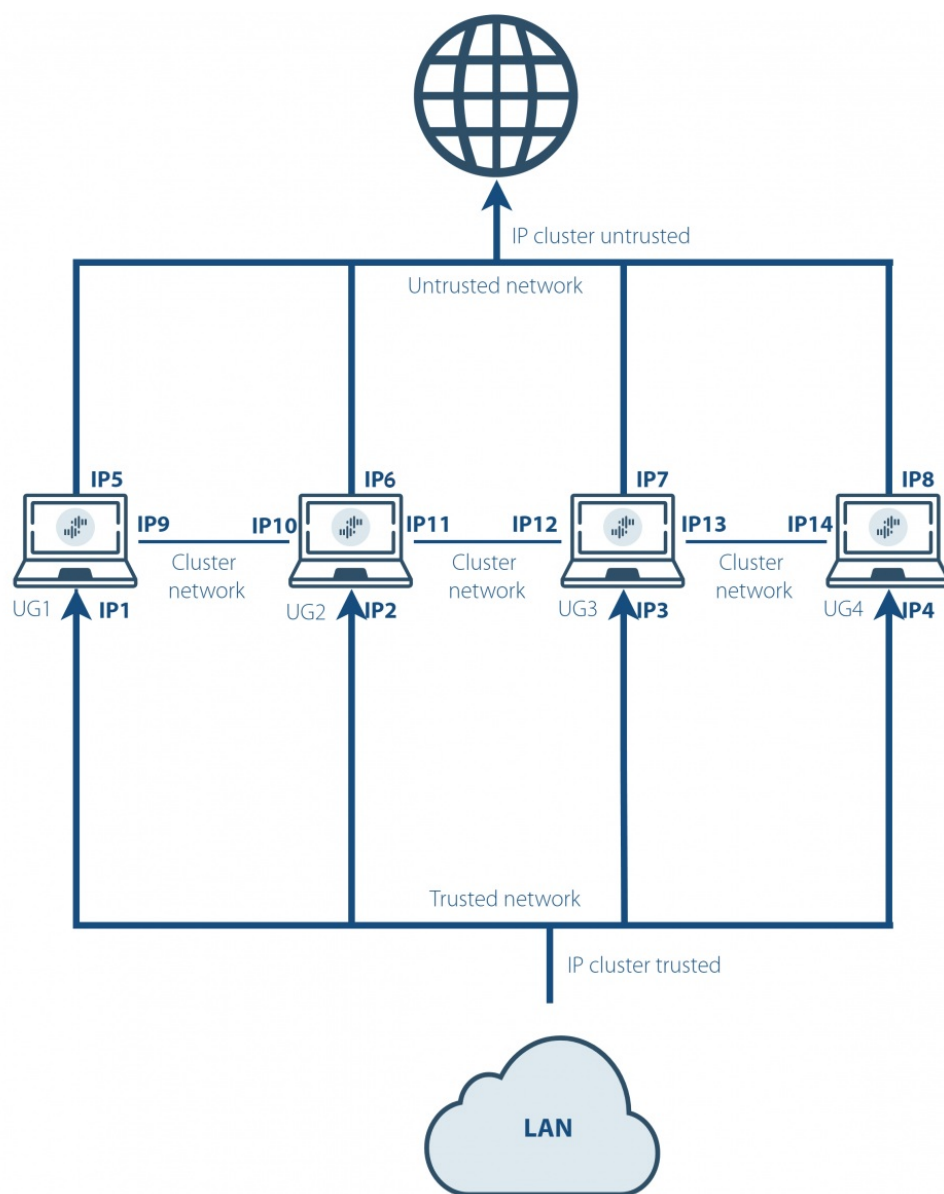
Примечание

Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на запасной узел при переключении, NGFW посылают служебное оповещение GARP (Gratuitous ARP), извещающий сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. В режиме Актив-Актив пакет GARP отсылается NGFW только при переходе роли мастера на запасной узел.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Актив**. Интерфейсы настроены следующим образом:

- **Зона Trusted:** IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Untrusted:** IP5, IP6, IP7, IP8 и IP cluster (Untrusted).
- **Зона Cluster:** IP9, IP10, IP11, IP12, IP13, IP14. Интерфейсы в зоне Cluster используются для репликации настроек.

Оба кластерных IP-адреса находятся на узле UG1. Если узел UG1 становится недоступным, то оба кластерных IP-адреса перейдут на следующий сервер, который станет мастер сервером, например, UG2.



Отказоустойчивый кластер в режиме Актив-Актив

Примечание Для корректной обработки трафика необходимо, чтобы обратный трафик от сервера к клиенту вернулся через тот же узел NGFW, через который он был инициирован от клиента, то есть, чтобы сессия пользователя всегда проходила через один и тот же узел кластера. Самое простое решение данной задачи - это использование NAT из сети клиента в сеть сервера (NAT из Trusted в Untrusted).

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать кластер конфигурации.	Создать кластер конфигурации, как это описано на предыдущем шаге.
Шаг 2. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере.	В разделе Зоны следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес (зоны Trusted и Untrusted на диаграммах выше).
Шаг 3. Создать кластер отказоустойчивости.	В разделе Управление устройством → Кластер отказоустойчивости нажать на кнопку Добавить и указать параметры кластера отказоустойчивости.
Шаг 4. Указать виртуальный IP-адрес для хостов auth.captive, logout.captive, block.captive, ftpclient.captive.	Если предполагается использовать авторизацию с помощью Captive-портала, то необходимо, чтобы системные имена хостов auth.captive и logout.captive, которые используются процедурами авторизации в Captive, резолвились в IP-адрес, назначенный в качестве кластерного виртуального адреса. Более детально эти параметры описаны в разделе Общие настройки .

Параметры отказоустойчивого кластера:

Наименование	Описание
Включено	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: • Актив-Актив — нагрузка распределяется на все узлы кластера. • Актив-Пассив — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.
Синхронизировать сессии	Включает режим синхронизации пользовательских сессий между всеми узлами, входящими в кластер отказоустойчивости. Включение данной опции делает переключение пользователей с одного устройства на другое прозрачным для пользователей, но добавляет существенную нагрузку на платформу NGFW. Имеет смысл только для режима кластера Актив-Пассив.
Мультикаст идентификатор кластера	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется определенный мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.
Идентификатор виртуального роутера (VRID)	Идентификатор виртуального роутера должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети не присутствуют сторонние кластеры VRRP, то рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Здесь же можно назначить роль Мастер-сервера одному из выбранных узлов.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера.

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

Доступ к веб-консоли NGFW регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети. Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

Примечание При первоначальной настройке NGFW создается локальный суперпользователь Admin.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора.	В разделе Администраторы → Профили администраторов нажать кнопку Добавить и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора.	В разделе Администраторы нажать кнопку Добавить и выбрать необходимый вариант: • Добавить локального администратора — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • Добавить пользователя LDAP — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы авторизации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • Добавить группу LDAP — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы авторизации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • Добавить администратора с профилем авторизации - создать пользователя, назначить созданный ранее профиль администратора и профиль авторизации (необходимы корректно настроенные серверы авторизации).

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Разрешения для API	Список объектов, доступных для делегирования доступа при работе через программный интерфейс (API). Объекты описаны документации API. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для веб-консоли	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для CLI	Позволяет разрешить доступ к CLI. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

Администратор NGFW может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей.	В разделе Администраторы → Администраторы нажать кнопку Настроить .
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: • Сложный пароль — включает дополнительные параметры сложности пароля, задаваемые ниже, такие как — минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. • Число неверных попыток аутентификации — количество неудачных попыток аутентификации администратора, после которых учетная запись блокируется на Время блокировки. • Время блокировки — время, на которое блокируется учетная запись.

ПримечаниеДополнительные параметры защиты учетной записи администратора применимы только к локальным учетным записям. Если в качестве администратора устройства выбирается учетная запись из внешнего каталога (например, LDAP), то параметры защиты для такой учетной записи определяются этим внешним каталогом.

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8001).

ПримечаниеНе рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети интернет.

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе **Контроль доступа** разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе [Настройка зон](#).

Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

Для включения данного режима необходимо выполнить следующие действия (в качестве примера используется утилита openssl):

Наименование	Описание
Шаг 1. Создать учетные записи дополнительных администраторов.	Произвести настройку, как это описано ранее в этой главе, например, создать учетную запись администратора с именем Administrator54.
Шаг 2. Создать или импортировать существующий сертификат типа УЦ авторизации веб-консоли.	Создать или импортировать существующий сертификат удостоверяющего центра (достаточно только публичного ключа) в соответствии с главой Управление сертификатами. Важно! Существующий сертификат удостоверяющего центра — сертификат, которым непосредственно подписаны сертификаты администраторов, а не корневой. Например, для создания УЦ с помощью утилиты openssl требуется выполнить команды: <pre>openssl req -x509 -subj '/C=RU/ST=Moscow/O= MyCompany /CN=ca.mycompany.com' -newkey rsa:2048 -keyout ca-key.pem -out ca.pem -nodes openssl rsa -in ca-key.pem -out ca-key.pem</pre> В файле ca-key.pem будет находиться приватный ключ сертификата, в ca.pem — публичный ключ. Импортировать публичный ключ в UserGate.
Шаг 3. Создать сертификаты для учетных записей администраторов.	С помощью средств сторонних утилит (например, openssl) создать сертификаты для каждого из администраторов. Необходимо, чтобы поле сертификата Common name в точности совпадало с именем учетной записи администратора, как она была создана в UserGate. Для openssl и пользователя Administrator54 команды будут следующими: <pre>openssl req -subj '/C=RU/ST=Moscow/O= MyCompany /CN=Administrator54' -out admin.csr -newkey rsa:2048 -keyout admin-key.pem -nodes</pre>

Наименование	Описание
Шаг 4. Подписать сертификаты администраторов, созданным на шаге 2 сертификатом удостоверяющего центра.	С помощью средств сторонних утилит (например, openssl) подписать сертификаты администраторов сертификатом удостоверяющего центра веб-консоли. Для openssl команды будут следующими: <pre>openssl x509 -req -days 9999 -CA ca.pem -CAkey ca-key.pem -set_serial 1 -in admin.csr -out admin.pem openssl pkcs12 -export -in admin.pem -inkey admin-key.pem -out admin.p12 -name 'Administrator54 client certificate'</pre> Файл admin.p12 содержит подписанный сертификат администратора.
Шаг 5. Добавить подписанные сертификаты в ОС, с которой администраторы будут авторизоваться в веб-консоль.	Добавить подписанные сертификаты администраторов (admin.p12 в нашем примере) в ОС (или в браузер Firefox, если он используется для доступа к консоли), с которой администраторы будут авторизоваться в веб-консоль. Более подробно смотрите руководство по используемой вами ОС.
Шаг 6. Переключите режим авторизации веб-консоли в авторизацию по сертификатам x.509.	В разделе Настройки поменяйте Режим авторизации веб-консоли на По X.509 сертификату.

ПримечаниеПереключить режим авторизации веб-консоли можно с помощью команд CLI.

В разделе **Администраторы → Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования NGFW. При необходимости любую из сессий администраторов можно сбросить (закрыть).

Общие сведения

UserGate использует защищенный протокол HTTPS для управления устройством, может перехватывать и дешифровать транзитный трафик пользователей, передаваемый по протоколу SSL (HTTPS, SMTPS, POP3S), а также может производить авторизацию администраторов в веб-консоль на основе их сертификатов.

Для выполнения данных функций NGFW использует различные типы сертификатов:

Наименование	Описание
SSL веб-консоли	Используется для создания безопасного HTTPS-подключения администратора к веб-консоли NGFW.
SSL Captive-портала	Используется для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. Этот сертификат должен быть выпущен со следующими параметрами: - Subject name — значение, установленное для домена Домен Auth captive-портала, определенного на странице Настройки. - Alternative names — необходимо указать все домены, для которых используется данный сертификат, как они заданы на странице Настройки: - домен Auth captive-портала. - домен Logout captive-портала. - домен страницы блокировки. - домен FTP поверх HTTP. - домен для веб-портала, указанный в настройках веб-портала. По умолчанию используется подписанный с помощью сертификата инспектирование SSL сертификат, выпущенный для домена auth.captive, со следующими параметрами: - Subject name = auth.captive - Alternative names = auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive Если администратор не загрузил свой собственный сертификат для обслуживания этой роли, то NGFW самостоятельно в автоматическом режиме перевыпускает данный сертификат при изменении администратором одного из доменов на странице Настройки (домены для auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive).
SSL инспектирование	Сертификат класса удостоверяющего центра. Он используется для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. Например, при перехвате HTTPS-трафика сайта yahoo.com оригинальный сертификат, выданный: Subject name = yahoo.com Issuer name = VeriSign Class 3 Secure Server CA — G3, подменяется на Subject name = yahoo.com Issuer name = компания, как она указана в сертификате центра сертификации, заведенного в NGFW. Данный сертификат также используется для создания сертификата по умолчанию для роли SSL Captive-портала.
SSL инспектирование (промежуточный)	Промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата.
SSL инспектирование (корневой)	Корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата.

Наименование	Описание
Пользовательский сертификат	Сертификат, который назначается пользователю NGFW. Пользователь может быть, как заведен локально, так и получен из LDAP. Сертификат может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси.
УЦ авторизации веб-консоли	Удостоверяющий центр авторизации администраторов для доступа к веб-консоли. Для успешной авторизации сертификат администратора должен быть подписан сертификатом этого типа.
SAML server	Используется для работы NGFW с сервером SSO SAML IDP. Подробно о настройке работы NGFW с сервером авторизации SAML IDP смотрите в соответствующем разделе руководства.
Веб-портал	Сертификат, используемый для веб-портала. Если данный сертификат не указан явно, то NGFW использует сертификат SSL Captive-портала, выпущенный сертификатом для инспектирования SSL. Подробно о настройке веб-портала смотрите в соответствующем разделе руководства.

Сертификатов для SSL веб-консоли, SSL Captive-портала и сертификатов SSL-инспектирования может быть несколько, но только один сертификат каждого типа может быть активным и использоваться для выполнения своих задач. Сертификатов типа УЦ авторизации веб-консоли может быть несколько, и каждый из них может быть использован для проверки подлинности сертификатов администраторов.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку Создать в разделе Сертификаты .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Страна — страна, в которой выписывается сертификат. • Область или штат — область или штат, в котором выписывается сертификат. • Город — город, в котором выписывается сертификат. • Название организации — название организации, для которой выписывается сертификат. • Common name — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • E-mail — email вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в NGFW. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата (SSL веб-консоли, инспектирование SSL, УЦ авторизации веб-консоли). В случае, если вы выбрали SSL веб-консоли, NGFW перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата. Сертификат инспектирования SSL начинает работать немедленно после того, как его выбрали. Более детально об инспектировании HTTPS смотрите в главе Инспектирование SSL .

NGFW позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов.

Наименование	Описание
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • Экспорт сертификата — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом читайте в Приложение 1. Установка сертификата локального удостоверяющего центра. • Экспорт CSR — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности NGFW не разрешает экспорт приватных ключей сертификатов.

ПримечаниеПользователи могут скачать себе для установки сертификат инспектирования SSL с NGFW по прямой ссылке: http://NGFW_IP:8002/cps/ca

Для импорта сертификата необходимо иметь файлы сертификата и — опционально — приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку Импорт .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Файл сертификата: загрузите файл, содержащий данные сертификата. • Приватный ключ: загрузите файл, содержащий приватный ключ сертификата. • Пароль для приватного ключа, если таковой требуется. • Цепочка сертификатов - файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

Использование корпоративного УЦ для создания сертификата инспектирования SSL

Если в компании уже существует внутренний УЦ или цепочка удостоверяющих центров, то можно указать в качестве сертификата для инспектирования SSL сертификат, созданный внутренним УЦ. В случае, если внутренний УЦ является доверяемым для всех пользователей компании, то перехват SSL будет происходить незаметно, пользователи не будут получать предупреждение о подмене сертификата.

Рассмотрим более подробно процедуру настройки NGFW. Допустим, что в организации используется внутренний УЦ на базе Microsoft Enterprise CA, интегрированный в Active Directory. Структура УЦ следующая:



Пример структуры корпоративного УЦ

Необходимо выпустить с помощью Sub CA2 сертификат для UserGate и настроить его в качестве сертификата для инспектирования SSL. Необходимо выпустить сертификат NGFW SSL decrypt в качестве удостоверяющего центра.

ПримечаниеNGFW не поддерживает алгоритм подписи rsassaPss. Необходимо, чтобы вся цепочка сертификатов, которая используется для выписывания сертификата для инспектирования SSL, не содержала данного алгоритма подписи.

Для выполнения этой задачи следует выполнить следующие шаги:

Наименование	Описание

Наименование	Описание
Шаг 1. Создать CSR-запрос на создание сертификата в UserGate.	Нажать на кнопку Создать → Новый CSR . Заполнить необходимые поля и создать CSR. Будет создан приватный ключ и файл запроса. С помощью кнопки Экспорт скачать файл запроса.
Шаг 2. Создать сертификат на основе подготовленного CSR.	В Microsoft CA создать сертификат на основе полученного на предыдущем шаге CSR-файла с помощью утилиты certreq: certreq.exe -submit -attrib "CertificateTemplate:SubCA" HTTPS_csr.pem или с помощью веб-консоли Microsoft CA, указав в качестве шаблона «Подчиненный центр сертификации». Обратитесь к документации Microsoft за более подробной информацией. По окончании процедуры вы получите сертификат (публичный ключ), подписанный УЦ Sub CA2.
Шаг 3. Скачать полученный сертификат.	Из веб-консоли Microsoft CA скачать созданный сертификат (публичный ключ).
Шаг 4. Загрузить сертификат в созданный ранее CSR.	В NGFW выбрать созданный ранее CSR и нажать кнопку Редактировать . Загрузить файл сертификата и нажать Сохранить .
Шаг 5. Указать тип сертификата - инспектирование SSL.	В NGFW выбрать созданный ранее CSR и нажать кнопку Редактировать . В поле Используется указать SSL инспектирование .
Шаг 6. Скачать сертификаты для промежуточных УЦ (Sub CA1 и Sub CA2).	В веб-консоли Microsoft CA выбрать и скачать сертификаты (публичные ключи) для УЦ Sub CA1 и Sub CA2.
Шаг 7. Загрузить сертификаты Sub CA1 и Sub CA2 в UserGate.	С помощью кнопки Импорт загрузить скачанные на предыдущем шаге сертификаты для Sub CA1 и Sub CA2.
Шаг 8. Установить тип — инспектирование SSL (промежуточный) для сертификатов Sub CA1 и Sub CA2.	В NGFW выбрать загруженные сертификаты и нажать кнопку Редактировать . Указать в поле Используется — Инспектирование SSL (промежуточный) для обоих сертификатов.
Шаг 9. Загрузить сертификат Root CA в NGFW (опционально).	С помощью кнопки Импорт загрузить корневой сертификат организации в NGFW. С помощью кнопки Редактировать указать в поле Используется — Инспектирование SSL (корневой) .

Интерфейс командной строки (CLI)

Version: 6.1.9
Product: UserGate NGFW
Documentation: ☒

UserGate позволяет создавать базовые настройки устройства с помощью интерфейса командной строки, или CLI (command line interface). С помощью CLI администратор может выполнить ряд диагностирующих команд, таких, как ping, nslookup, traceroute, осуществить настройку сетевых интерфейсов и зон, а также перезагрузить или выключить устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании UserGate), через последовательный порт или с помощью SSH по сети.

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к UserGate.	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — utm.

ПримечаниеДля работы с интерфейсом командной строки с ПО версий 6.1.x нельзя использовать пароль администратора, в котором после одного символа \$ будут любые другие символы, например, \$pass123 или pass123\$. Если после символа \$ не будет ничего, то пароль будет работать, например, pass123\$.

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к UserGate.	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate.
Шаг 2. Запустить терминал.	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — utm.

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны.	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал.	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UserGate, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: ssh Admin@IPUserGate -p 2200

Наименование	Описание
Шаг 3. Войти в CLI.	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — utm.

После успешного входа в CLI можно посмотреть список возможных команд с помощью команды **help**. Для подробного описания любой команды необходимо использовать синтаксис

help command

Например, для получения подробной справки по использованию команды настройки сетевого интерфейса iface необходимо выполнить

help iface

Полный список команд:

Наименование	Описание
help	Показывает список доступных команд.
exit quit Ctrl+D	Выйти из CLI.
cache ldap-clear	Очистка кэша LDAP-записей.
code-change-control	Набор команд для просмотра и настройки параметров защиты исполняемого кода продукта от потенциального несанкционированного изменения. Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate. code-change-control show — показывает текущий режим работы. По умолчанию отслеживание несанкционированных изменений исполняемого кода отключено. code-change-control set log — активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. code-change-control set block — активирует режим отслеживания несанкционированных изменений исполняемого кода. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений. code-change-control set off — отключает режим отслеживания несанкционированных изменений исполняемого кода. Требуется указания пароля, который был задан при активации режима отслеживания исполняемого кода.
config-change-control	Набор команд для просмотра и настройки параметров защиты конфигурации (настроек) продукта от изменения. Перед активацией защиты конфигурации администратор производит настройку продукта в соответствии с требованиями организации, после чего "замораживает" настройки (режим log или block). Любое изменение настроек через веб-интерфейс, CLI или другими способами будет приводить к журналированию и/или блокировке транзитного трафика, в зависимости от выбранного режима. Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate. config-change-control show — показывает текущий режим работы. По умолчанию отслеживание изменений конфигурации отключено. config-change-control set log — активирует режим отслеживания изменений конфигурации. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. config-change-control set block — активирует режим отслеживания изменений конфигурации. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для отключения созданного правила межсетевого экрана необходимо сбросить состояние блокировки с помощью следующей команды: config-change-control set off — отключает режим отслеживания изменений конфигурации. Требуется указания пароля, который был задан при активации режима отслеживания конфигурации.

Наименование	Описание
date	Посмотреть текущее время на сервере.
device	Набор команд для изменения параметров устройства. • device passwd — позволяет сменить пароль пользователю, залогиненному в CLI-консоль. • device config -list — показывает список доступных опций для настройки. • device config -get — посмотреть текущее значение параметра. • device config -set — изменить значение параметра. Список доступных параметров: • module_l7_enabled — включение/отключение загрузки модуля L7. По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка устройства UserGate. • module_idps_enabled — включение/отключение загрузки модуля idps. По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка устройства UserGate. • module_h323_enabled — включение/отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT. По умолчанию модуль выгружен. • fw_drop_invalid — включение/отключение блокировки пакетов с невалидным набором параметров в полях заголовка. Включение данной опции существенно понижает производительность межсетевого экрана. Рекомендуется оставить данную настройку в выключенном состоянии. • fw_established — включение/отключение создания одного общего правила межсетевого экрана для обратных пакетов. • module_sip_enabled — включение/отключение загрузки модуля sip; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT. По умолчанию модуль выгружен. • module_sunrpc_enabled — включение/отключение загрузки модуля sunrpc. По умолчанию модуль выгружен. • module_ftp_alg_enabled — включение/отключение загрузки модуля ftp; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT. По умолчанию модуль выгружен. Важно! Модуль нужно включать для пассивного режима работы FTP. • fastpath — включение/отключение модуля ускоренной обработки сетевого трафика. По умолчанию данная настройка включена. В случае отключения модуля ускоренной обработки сетевого трафика, модуль будет снова включен при перезагрузке устройства. • ha_auth_type — включение подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости. Для включения подписи необходимо использовать команду: device config -set ha_auth_type ah Для отключения проверки: device config -set ha_auth_type pass
gateway	Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации.
iface	Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации. Следующие параметры команды iface позволяют управлять пересылкой пакетов directed broadcast, приходящих на указанный интерфейс: <pre>iface config -name port X -link-info 'bc_forwarding=1' -enabled true</pre> <pre>iface config -name port X -link-info 'bc_forwarding=1' -enabled false</pre> Следующие параметры команды iface включают механизм Proxy ARP, UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса: <pre>iface config -name port X -link-info 'proxy_arp=1' -enabled true</pre> Следующие параметры команды iface включают механизм Proxy ARP, UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса: <pre>iface config -name port X -link-info 'proxy_arp_pvlan=1' -enabled true</pre>

Наименование	Описание
license	Посмотреть информацию о лицензии.
netcheck	Проверить доступность стороннего HTTP/HTTPS-сервера. netcheck [-t TIMEOUT] [-d] URL Опции: -t - максимальный таймаут ожидания ответа от веб-сервера -d - запросить содержание сайта. По умолчанию запрашиваются только заголовки.
node	Набор команд для просмотра и настройки узлов кластера. Смотрите node help для детальной информации.
nslookup	Выполнить определение IP-адреса по имени хоста.
ping	Выполнить ping определенного хоста.
proxy	Набор команд для просмотра и настройки параметров прокси-сервера. Позволяет настроить такие параметры, как добавление заголовков HTTP — via и forwarded, а также настройки таймаутов на подключение к сайтам и на загрузку контента: • add_via_enabled - добавлять HTTP заголовок via. По умолчанию отключено. • add_forwarded_enabled - добавлять HTTP заголовок forwarded. По умолчанию отключено. • add_xforwarded_enabled — добавлять HTTP заголовок X-Forwarded-For. По умолчанию отключено. • http_connection_timeout - время ожидания, выделяемое на подключение http. По умолчанию — 20 секунд. • http_loading_timeout - время ожидания, выделяемое на загрузку контента http. По умолчанию — 60 секунд. • proxy_host_rfc — разрешить использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. По умолчанию установлено значение strict (соблюдать RFC). • fmode_enabled (boolean) — включает режим ускорения загрузки контента. Может быть несовместим с работой некоторых сайтов. По умолчанию отключен. • icap_wait_timeout — время в секундах, которое сервер UserGate ждет ответа от ICAP-сервера. Если ответ сервера не был получен в заданный промежуток времени, то в случае, если действие правила Переслать и игнорировать, UserGate отправит данные пользователю без модификации, если же действие правила Переслать, UserGate не отдаст данные пользователю. Значение по умолчанию — 10 секунд. • smode_enabled (boolean) - включает режим SYN Proxy. По умолчанию выключен. • legacy_ssl_enabled (boolean) - отключает поддержку дешифрования протокола SSL TLSv1.3. При включении данного режима UserGate поддерживает работу протоколов TLSv1.0-TLSv1.2. Если режим отключен, то поддерживается работа только TLSv1.0-TLSv1.3. По умолчанию отключен. Рекомендуется не изменять значения по умолчанию. Смотрите proxy help для детальной информации.
radmin	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate.
radmin_e	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate, в случаях, когда сервер UserGate завис. В случаях, когда произошла проблема с ядром UserGate, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации UserGate. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.
reboot	Перезагрузить сервер UserGate.
route	Создать, изменить, удалить маршрут.
shutdown	Выключить сервер UserGate.

Наименование	Описание
telemetry	Набор команд для просмотра и настройки режима работы телеметрии. Телеметрия позволяет отправлять разработчику анонимную статистику, такую как, популярность веб-сайтов, веб-сайты с неизвестной категорией, вирусные атаки, события COB, активность малваре. Данные телеметрии имеют вид обезличенных данных и не содержат персональную информацию. Отправка телеметрии активирована по умолчанию. telemetry show - показать текущий режим. telemetry set -enabled true - активировать телеметрию. telemetry set -enabled false - отключить отсылку телеметрической информации.
traceroute	Выполнить трассировку соединения до определенного хоста.
usersession	Команда для сброса авторизации указанного пользователя. usersession terminate -ipv4 IP_ADDRESS - сбрасывает авторизацию для указанного IP_ADDRESS.
webaccess	Набор команд для просмотра режима авторизации веб-консоли. Позволяет вернуть режим По имени и паролю при невозможности авторизоваться с помощью сертификатов.
zone	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

Version: 5.x, 6.1.9
Documentation: ☒

Системные утилиты доступны администратору во время загрузки сервера UserGate через меню загрузки (boot menu). Для получения доступа к этому меню необходимо подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB (при наличии соответствующих разъемов на устройстве) или используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate. Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

Во время загрузки администратор может выбрать один из нескольких пунктов загрузки в boot-меню:

Наименование	Описание
1. UserGate (serial console)	Загрузка UserGate с выводом диагностической информации о загрузке в последовательный порт.
2. UserGate (verbouse mode)	Загрузка UserGate с выводом диагностической информации о загрузке в консоль tty1 (монитор).
3. Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
4. Support menu (serial console)	Войти в раздел системных утилит с выводом информации в последовательный порт. При подключении через последовательный порт загрузочное меню не отображается. Для выбора раздела Support menu необходимо во время загрузки нажимать клавишу "4". Для выбора одного из пунктов меню в разделе Support menu необходимо нажать клавишу, соответствующую первой букве названия пункта меню, например, для выбора Restore backup , необходимо нажать клавишу " R ", затем клавишу " Ввод ".
5. Memory test	Запуск проверки оперативной памяти устройства.

Раздел системных утилит (Support menu) позволяет выполнить следующие действия:

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Clear logs	Очистка диагностических журналов для освобождения пространства на системном разделе. Журналы UserGate не очищаются (журналы веб-доступа, трафика, событий, COB и т.п.).
Export logs	Выгрузка диагностических журналов на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Expand log partition	Увеличение раздела для журналов на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate. Данные и настройки UserGate не сбрасываются.
Backup full	Создать полную копию диска UserGate на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Backup system only	Создать копию системного раздела UserGate, исключая журналы (журналы веб-доступа, трафика, событий, COB и т.п.) на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate с внешнего USB носителя.
Update from USB	Установка обновления ПО UserGate с внешнего USB носителя. Обновление должно быть скопировано в корень съемного диска, диск должен иметь формат NTFS или FAT32. Название файла обновления должно быть в следующем формате: update_XXXXX (где XXXXX - номер сборки). Без расширения .bin.

Наименование	Описание
Refresh NIC names	Упорядочивание имен сетевых портов в необходимом порядке. Упорядочивание производится в соответствии с номером порта на шине PCI. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UserGate не сбрасываются.
Factory reset	Сброс состояния UserGate к первоначальному состоянию системы. Версия ПО вернется к той, которая была при первоначальной установке. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

