

Table of Contents

Table of Contents	1
Настройка устройства	2
Настройка общих параметров	3
Управление устройством	6
Управление доступом к веб-консоли UserGate WAF	10
Управление сертификатами	13
Профили клиентских сертификатов	15
Системные утилиты	16
Расширение системного раздела	17
Кластеризация и отказоустойчивость	18

Настройка общих параметров

Version: 7.7.x

Product: WAF

В этом разделе описаны общие параметры UserGate WAF, которые отображаются на странице веб-консоли **Настройки** в разделе **Консоль администратора** → **Настройки**, а также приведены рекомендации по настройке этих параметров.

Блок параметров	Параметр	Описание
Настройки интерфейса	Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Используется для работы расписаний, настроенных в правилах, а также для корректного отображения времени и даты, например в отчетах или в журналах
	Язык интерфейса по умолчанию	Язык, используемый в веб-консоли устройства по умолчанию
	Режим аутентификации веб-консоли	Доступны следующие режимы аутентификации: • По имени и паролю. Вход администратора в веб-консоль по логину и паролю учетной записи. • По X.509-сертификату. Вход администратора в веб-консоль по цифровому сертификату. Этот сертификат должен быть подписан сертификатом удостоверяющего центра, обеспечивающим доступ к веб-консоли, и установлен в браузере. При включении режима отключается аутентификация по логину и паролю, к ней можно вернуться с помощью команд CLI. • Профиль клиентского сертификата. Вход администратора в веб-консоль по сертификату инфраструктуры открытых ключей (PKI). Проверка подлинности этого сертификата выполняется с помощью профиля клиентского сертификата, обеспечивая тем самым безопасность сетевого соединения
	Профиль SSL для веб-консоли	Профиль SSL , с использованием которого создается защищенный канал для доступа к веб-консоли
	Таймер автоматического закрытия сессии (мин.)	Для настройки таймера необходимо указать, по истечении скольких минут бездействия администратора в веб-консоли должна завершаться его сессия. Также необходимо включить параметр Автоматическое закрытие сессии по таймеру
	Автоматическое закрытие сессии по таймеру	При включенном параметре сессия администратора будет завершаться по истечении таймера автоматического закрытия сессии По умолчанию параметр отключен
Настройка времени сервера	Использовать NTP	При включенном параметре для синхронизации времени на устройстве будут использоваться NTP-серверы из указанного списка
	Основной NTP-сервер	Адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org
	Запасной NTP-сервер	Адрес запасного сервера точного времени
	Время на сервере (UTC)	Время на сервере UserGate WAF в часовом поясе UTC
	Канал обновлений	Настройка канала для получения обновлений программного обеспечения UserGate (UGOS) из репозитория UserGate. Вы можете выбрать Стабильные (стабильные версии ПО) или Бета (версии ПО для бета-тестирования). Если настроена интеграция с UserGate Management Center, параметр примет значение Management Center и будет недоступен для изменения

Обновления параметров	Параметр	Описание
	Обновления	Проверка наличия обновлений UGOS в репозитории UserGate. После проверки вы можете вручную загрузить и установить доступные обновления. В процессе установки обновления UGOS вы можете создать точку восстановления. Это позволит восстановить предыдущую версию UGOS при возникновении проблем. Действие будет доступно в стартовом меню после установки обновления UGOS
	Офлайн-обновление	Загрузка файла обновления UGOS офлайн
Обновления библиотек	Обновления	Проверка наличия обновлений системных библиотек, предоставляемых по подписке, в репозитории UserGate. После проверки вы можете вручную обновить необходимые библиотеки
	Расписание автоматических обновлений	Настройка расписания автоматического обновления библиотек. При настройке расписания вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Для ручного ввода вы можете использовать следующие символы: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями. При установке флажка Единое расписание для всех обновлений расписание выбранной библиотеки будет применено ко всем библиотекам в списке. Примечание В целях уменьшения нагрузки на систему рекомендуется настраивать расписание автоматического обновления только для используемых библиотек
Модули	Настройка LLDP	Настройка использования LLDP-протокола канального уровня, с помощью которого UserGate WAF обменивается данными с соседними устройствами в локальной сети. Для настройки доступны следующие параметры: Transmit delay — интервал отправки LLDP-пакетов (от 1 до 3600 секунд). Изменяя этот параметр, вы можете управлять частотой, с которой UserGate WAF будет отправлять данные соседним устройствам. Transmit hold — множитель для вычисления времени жизни LLDP-пакетов (параметр TTL). Укажите значение (от 1 до 100), на которое следует умножить значение Transmit delay, чтобы определить время хранения данных, полученных от соседних устройств. По истечении этого времени данные удаляются из кэша UserGate WAF. Для использования LLDP-протокола необходимо предварительно создать LLDP-профиль и назначить его сетевому интерфейсу устройства. Список соседних LLDP-устройств отображается в разделе веб-консоли Диагностика и мониторинг → Сеть → LLDP-соседи (см. раздел «LLDP-соседи»)
Log Analyzer	Сервер	Сервер базы данных журналов. Может быть указан локальный сервер или внешний сервер UserGate Log Analyzer или UserGate SIEM
	Версия сервера	Версия ПО сервера базы данных журналов
	Версия устройства	Версия ПО UserGate WAF
	Код устройства	Уникальный код UserGate WAF для интеграции с внешним сервером UserGate Log Analyzer или UserGate SIEM

Блок параметров	Параметр	Описание
Агент UserGate Management Center	Настройка агента	Настройка агента для интеграции с UserGate Management Center (UGMC). Для настройки доступны следующие параметры: • Включено — управление состоянием подключения UserGate WAF к UGMC. • Адрес сервера UserGate Management Center — адрес сервера UGMC в формате IPv4-адреса или FQDN (возможно использование IDN-адреса). • Код устройства — идентификатор UserGate WAF для подключения к UGMC
Серверы DNS	Системные DNS-серверы	Настройка IP-адресов DNS-серверов

Version: 7.7.x
Product: WAF

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

- параметры диагностики;
- операции с сервером;
- резервное копирование;
- экспорт и импорт настроек.

Диагностика

Этот блок предназначен для настройки параметров диагностики и предоставления удаленного доступа службе технической поддержки UserGate с целью анализа и устранения неисправностей.

Параметры диагностики

С помощью параметра **Детализация диагностики** вы можете установить уровень журналирования устройства. Доступны следующие уровни:

- **Off** — ведение журналов диагностики отключено.
- **Error** — журналировать только ошибки в работе устройства.
- **Warning** — журналировать только ошибки и предупреждения.
- **Info** — журналировать только ошибки, предупреждения и дополнительную информацию.
- **Debug** — журналировать все возможные события.

При журналировании с уровнями **Warning**, **Info** и **Debug** может снижаться производительность устройства, поэтому рекомендуется устанавливать уровни **Error** или **Off**, если технической поддержкой UserGate не было предложено иное.

Управление журналами диагностики

Вы можете скачать диагностические журналы для их передачи в службу технической поддержки UserGate. Для скачивания доступны журналы веб-консоли и системные журналы. Скачать выбранные журналы можно после их архивирования командой **Начать архивирование журналов**.

Чтобы удалить архивные (не активные в настоящий момент) журналы, нажмите **Очистить файлы логов**.

Удаленный помощник

Чтобы предоставить доступ к устройству для службы технической поддержки UserGate с целью диагностирования и устранения неисправностей, необходимо активировать функцию удаленного помощника и получить параметры сеансового доступа.

Процесс подключения к устройству происходит следующим образом:

1. Администратор устройства UserGate активирует функцию удаленного помощника.
2. Устройство устанавливает защищенное соединение с сервером удаленного помощника UserGate по протоколу SSH. При успешном подключении в интерфейсе устройства UserGate отобразятся параметры сеансового доступа: идентификатор и токен.
3. Администратор устройства UserGate передает параметры сеансового доступа специалисту технической поддержки UserGate.
4. Специалист технической поддержки устанавливает защищенное соединение по протоколу SSH с сервером удаленного помощника UserGate и с помощью параметров сеансового доступа подключается к устройству UserGate.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• Перезагрузить — перезагрузка WAF. • Выключить — выключение WAF

Наименование	Описание
Проверка лицензии и обновлений вышестоящим прокси-сервером	Настройка параметров вышестоящего HTTP(S) прокси-сервера для обновления лицензии и обновления ПО WAF. Необходимо указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на вышестоящем прокси-сервере

Команда UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта 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 WAF.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния WAF, 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 WAF будет перезагружен

Управление резервным копированием

Данный раздел позволяет управлять резервным копированием UserGate WAF: настройка правил экспорта конфигурации, создание резервной копии, восстановление UserGate WAF.

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать резервную копию	В разделе Управление устройством → Управление резервным копированием нажать Создание резервной копии. Система сохранит текущие настройки сервера под следующим именем: backup_PRODUCT_NODE-NAME_DATE.gpg, где: <i>PRODUCT</i> — тип продукта: WAF, LogAn, MC; <i>NODE-NAME</i> — имя узла UserGate; <i>DATE</i> — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC. Процесс создания резервной копии может быть прерван нажатием кнопки Остановить. Запись о создании резервной копии отобразится в журнале событий устройства

Для восстановления состояния устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Восстановить состояние устройства	В разделе Управление устройством → Управление резервным копированием нажать Восстановление из резервной копии и указать путь к ранее созданному файлу настроек для его загрузки на сервер. Восстановление будет предложено в консоли tty при перезагрузке устройства

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

Наименование	Описание

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе Управление устройством → Управление резервным копированием 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/Повторите пароль — пароль учетной записи. • Путь на сервере — путь на сервере, куда будут выгружены настройки. Путь на сервере должен уже существовать. Сама <u>система</u> несуществующие папки <u>не создаст</u>! В случае использования SSH-сервера возможно использование авторизации по ключу. Для импорта или генерации ключа необходимо выбрать Настроить SSH-ключ и указать Сгенерировать ключи или Импортировать ключ. Важно! При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен находиться на SSH-сервере в директории пользовательских ключей /home/user/.ssh/ в файле authorized_keys. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка Проверить соединение); при проверке соединения fingerprint помещается в known_hosts, без проверки файлы не будут отправляться. Важно! Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга
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"

Экспорт и импорт настроек

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

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 всех интерфейсов.
- Настройки шлюзов.
- Настройки виртуальных маршрутизаторов (VRF).
- Настройки зон.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание

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

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

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"

Version: 7.7.x
Product: WAF

Доступ к веб-консоли UserGate WAF 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 UserGate WAF 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 аутентификации - 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 доступа	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 UserGate WAF 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 заблокируется 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**. Подробнее о настройке контроля доступа к зонам — в разделе « [Настройка сетевых 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 (удостоверяющего центра) 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 удостоверяющего центра 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 WAF
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 WAF. 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 аутентификации веб-консоли в авторизацию по сертификатам x.509.	В разделе Настройки поменяйте Режим аутентификации 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 UserGate WAF. При необходимости любую из сессий администраторов можно сбросить (закрыть).

Product: WAF
Version: 7.7.x

Общие сведения

UserGate WAF использует защищенный протокол HTTPS для управления устройством, а также может производить авторизацию администраторов в веб-консоль на основе их сертификатов.

Для выполнения данных функций UserGate WAF использует различные типы сертификатов:

Наименование	Описание
SSL веб-консоли	Используется для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate WAF
УЦ для авторизации в веб-консоли	Сертификат удостоверяющего центра для доступа к веб-консоли. Для успешной авторизации сертификат администратора должен быть подписан сертификатом этого типа
SAML server	Используется для работы UserGate WAF с сервером SSO SAML IDP. Подробно о настройке работы UserGate WAF с сервером авторизации SAML IDP смотрите в соответствующем разделе руководства

Сертификатов для SSL веб-консоли может быть несколько, но только один сертификат каждого типа может быть активным и использоваться для выполнения своих задач. Сертификатов типа **УЦ для авторизации в 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 UserGate WAF. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата (SSL веб-консоли, УЦ для авторизации в веб-консоли). В случае, если вы выбрали SSL веб-консоли, UserGate WAF перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата

UserGate WAF 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

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов
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 установки его в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом читайте в приложении «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 UserGate не разрешает экспорт приватных ключей сертификатов.

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

Профили клиентских сертификатов

Version: 7.7.x

Product: WAF

Профиль клиентского сертификата позволяет управлять сертификатами для обеспечения безопасности и подтверждения подлинности в сетевых соединениях. В профиле указываются сертификаты УЦ, методы проверки актуальности пользовательских сертификатов, методы выбора имени пользователя для аутентификации.

Профиль клиентского сертификата используется для валидации предоставленного клиентом сертификата. Сертификат клиента проверяется на валидность для каждого сертификата УЦ из списка.

При выборе режима аутентификации посредством сертификатов (PKI) указывается сконфигурированный ранее профиль клиентского сертификата, который в дальнейшем можно будет использовать в настройках reverse-прокси.

Чтобы создать профиль клиентского сертификата, необходимо в разделе **Настройки → Консоль администратора → Профили клиентских сертификатов** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля клиентских сертификатов
Описание	Оptionальное описание профиля
Получать имя пользователя из	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • Common-name — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат. • Subject altname email — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name). • Principal name — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. Если в полях расширения SAN сертификата указано несколько имен UPN или несколько электронных адресов, берется первый, указанный в сертификате
Сертификаты УЦ	Сертификаты УЦ, назначаемые профилю. Список сертификатов удостоверяющих центров. Используется для валидации предоставленного клиентом сертификата. Сертификат клиента проверяется на валидность для каждого сертификата УЦ из списка. Перебор списка идет сверху вниз
Проверка отозванных сертификатов	В списках отзыва сертификатов (CRL) содержатся сертификаты, которые были отозваны и больше не могут использоваться. В этот список входят сертификаты, срок действия которых истек или они были скомпрометированы. Параметр для проверки состояния отзыва сертификатов: • Не проверять — не проверять ни один сертификат. • Вся цепочка — проверять все сертификаты в цепочке и требовать, чтобы они все были валидными. • Сертификат пользователя — проверять только сертификат клиента. • Считать валидным, если статус неизвестен — если проверить CRL не удалось по какой-то причине, то сертификат считается валидным (при этом он всё равно проверяется и может вернуть статус invalid, если сертификат есть в списке отозванных)
Тайм-аут проверки	Интервал времени, по истечению которого UserGate WAF перестает ожидать ответа от службы списков отзыва сертификатов

Системные утилиты

Version: 7.7.x
Product: WAF

Системные утилиты доступны администратору во время загрузки UserGate WAF 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 WAF. 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
UGOS WAF	Загрузка UserGate WAF с выводом диагностической информации о загрузке в последовательный порт
UGOS WAF (failsafe)	Загрузка UserGate WAF в упрощённом видеорежиме
Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор)
Restore previous version	Раздел доступен после обновления или создания резервной копии

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
Expand data partition	Увеличение раздела для хранения данных. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate WAF. Важно! Для расширения системного раздела с сохранением данных и параметров UserGate WAF необходимо средствами гипервизора добавить новый диск и затем выполнить операцию Expand data partition , как описано в разделе « Расширение системного раздела »
Create backup	Создать полную копию диска UserGate WAF на внешний USB носитель. Важно! Перед созданием резервной копии USB носитель будет отформатирован
Restore from backup	Восстановление UserGate WAF с внешнего USB носителя
Factory reset	Сброс состояния UserGate WAF. Версия ПО останется той, которая была установлена при запуске команды. Все данные и настройки будут утеряны
Exit	Выход и перезагрузка устройства

Расширение системного раздела

Version: 7.7.x
Product: WAF

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить новый диск необходимого размера в свойствах виртуальной машины UserGate
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate войти в раздел Support menu В открывшемся разделе выбрать Expand data partition и запустить процесс расширения раздела
Шаг 3. Проверить размер системного раздела.	После завершения процесса расширения загрузить узел и в разделе Дашборд → Диски проверить размер системного раздела

Примечание Расширение системного раздела путем увеличения размера имеющегося диска виртуальной машины возможно только при сбросе узла до заводских настроек, т.е. при выполнении операции factory reset.

Technology: Clustering and HA

Version: 7.7.x

Product: WAF

Для построения отказоустойчивого решения UserGate WAF необходимо настроить два типа кластеров — кластер конфигурации и кластер отказоустойчивости:

- **Кластер конфигурации.** Узлы, объединенные в одну общую схему, «видят» друг друга и синхронизируют свою конфигурацию, поддерживая таким образом единые параметры фильтрации и обработки трафика в рамках кластера. Такая синхронизация гарантирует, что набор политик будет одинаковым на всех узлах кластера и все изменения конфигурации будут выполняться с минимальными задержками. При этом часть параметров для каждого из узлов кластера остается уникальной, например параметры сетевых интерфейсов, шлюзов, маршрутов и диагностики.
- **Кластер отказоустойчивости.** Если в сети настроен кластер конфигурации, то до четырех узлов, входящих в него, можно объединить в кластер отказоустойчивости, который обеспечит непрерывную фильтрацию и обработку трафика. В дополнение к возможностям кластера конфигурации кластер отказоустойчивости поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла кластера на другой, — за исключением сессий, использующих прокси-сервер, например трафик HTTP(S). Вы можете собрать несколько кластеров отказоустойчивости. Например, если в кластер конфигурации добавлены узлы A, B, C и D, на их основе можно создать два кластера отказоустойчивости — A-B и C-D.

Важно! Работа устройств UserGate в режимах кластера конфигурации и кластера отказоустойчивости доступна, если в используемую лицензию включен модуль Cluster.

Настройка кластера конфигурации

Настройка кластера конфигурации состоит из двух этапов: настройки первого узла и добавления дополнительных узлов. Каждый дополнительный узел добавляется в кластер на этапе первоначальной настройки этого узла. Если в вашей сети уже есть устройства UserGate WAF, работающие как независимые, их можно добавить в кластер только выполнив сброс к заводским параметрам.

Чтобы настроить кластер конфигурации:

1. Выполните [первоначальную настройку](#) первого узла кластера. Убедитесь, что активированная лицензия на первом узле (раздел **Дашборды** → **Лицензия**) включает в себя модуль Cluster.
 2. В веб-консоли первого узла в разделе **Настройки** → **Сеть** → **Зоны** добавьте зону, в которой будет выполняться репликация кластера, или выберите существующую зону **Cluster**. Убедитесь, что для выбранной зоны в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешены сервисы **Консоль администрирования** и **Кластер**.

Важно! Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например к интернету.
 3. В разделе **Настройки** → **Сеть** → **Интерфейсы** выберите интерфейс, через который будет выполняться репликация кластера, и нажмите **Редактировать**.
 4. В окне **Свойства интерфейса**:
 - на вкладке **Общие** назначьте интерфейсу зону кластера и установите флажок **Включено**;
 - на вкладке **Сеть** выберите режим **Статический**, с помощью кнопки **Добавить** укажите IP-адрес;
 - нажмите **Сохранить**.
 5. В разделе **Настройки** → **Консоль администратора** → **Управление устройством** → **Кластер конфигурации** выберите текущий узел кластера, нажмите **Редактировать**, укажите IP-адрес, назначенный интерфейсу на предыдущем шаге и нажмите **Сохранить**. Начнется перезагрузка устройства.
 6. После завершения перезагрузки в блоке **Кластер конфигурации** выберите текущий узел, нажмите **Сгенерировать секретный код** и скопируйте код для авторизации дополнительного узла кластера.
 7. Подключитесь к веб-консоли дополнительного узла. В мастере первоначальной настройки выберите язык интерфейса, примите лицензионное соглашение и затем в окне **Установка** нажмите **Установка дополнительного узла кластера**.
 8. В блоке **Шаг 1** укажите параметры дополнительного узла: кластерный интерфейс, его IP-адрес, маску подсети и IP-адрес шлюза (в случае, если первый и дополнительный узлы кластера находятся в разных подсетях). Например, если оба узла находятся в одной подсети, кластерному интерфейсу eth2 первого узла может быть назначен IP-адрес 192.168.100.5/24, а интерфейсу eth2 дополнительного узла в этом случае можно назначить IP-адрес 192.168.100.6/24.
- Примечание** Так как IP-адрес интерфейса дополнительного узла и шлюз по умолчанию на этом шаге указываются в явном виде, режим присвоения этих параметров будет статическим.
9. В блоке **Шаг 2** укажите IP-адрес кластерного интерфейса первого узла, вставьте созданный на нем секретный код и нажмите **Подключить**. Начнется настройка дополнительного узла, после чего он будет добавлен в кластер и все параметры первого узла реплицируются на дополнительный.
 10. В веб-консоли дополнительного узла кластера конфигурации в разделе **Настройки** → **Сеть** → **Интерфейсы** назначьте каждому интерфейсу корректную зону, так как текущие параметры были получены в результате репликации данных с первого узла кластера.
 11. В веб-консоли дополнительного узла кластера конфигурации на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**, чтобы активировать лицензию на дополнительном узле.

Примечание Если на первом узле кластера лицензия была активирована онлайн, дополнительному узлу для активации лицензии также потребуется доступ в интернет. При офлайн-активации лицензии на первом узле подключение дополнительного узла к интернету не требуется.

12. Настройте шлюзы, маршруты, параметры OSPF, BGP, уникальные для каждого из узлов.

Примечание К уникальным относятся параметры диагностики, интерфейсов, шлюзов, DHCP, маршрутов, OSPF и BGP.

Вы можете отслеживать состояние узлов кластера конфигурации по статусу узла UserGate в любой из веб-консолей в блоке **Настройки → Консоль администратора → Управление устройством → Кластер конфигурации**:

- Зеленый: узел доступен.
- Оранжевый: узел недоступен, идет перезагрузка узла.
- Красный: узел недоступен, связь с узлом потеряна.
- Черный: идет запуск узла.

О кластере отказоустойчивости

В режиме работы кластера «активный — пассивный» одно из устройств выступает в роли мастер-узла (в веб-консоли статус этого узла — master), а остальные — в качестве резервных (в веб-консоли статус этих узлов — backup). Узел, выбранный в качестве мастер-узла, обладает наивысшим приоритетом в кластере, он отвечает на ARP-запросы клиентов и выполняет обработку и инспектирование пользовательского трафика. Резервные узлы не обрабатывают трафик, поступающий на виртуальные IP-адреса кластера, и находятся в режиме ожидания. При этом узлы, выступающие в кластере в роли резервных, могут обрабатывать трафик, который передается на их интерфейсы, не являющиеся кластерными.

На каждом из узлов кластера по умолчанию выбраны сетевые интерфейсы в зоне Cluster, которым назначены кластерные IP-адреса. Между кластерными интерфейсами передаются VRRP-объявления — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии. На основании VRRP-объявлений оценивается связность кластера, и уточняются приоритеты всех узлов кластера. Также кластерные интерфейсы участвуют в синхронизации сессий между узлами кластера.

На другие сетевые интерфейсы узлов кластера назначаются виртуальные IP-адреса, на которые направляется трафик. В случае если мастер-узел стал недоступен, роль мастер-узла и все виртуальные IP-адреса переносятся на резервный узел с наибольшим IP-адресом либо — если настроены необходимые параметры — с наибольшим приоритетом. Этот узел продолжит обработку трафика.

Безусловный перенос роли мастер-узла на резервный узел происходит при следующих событиях:

- Резервный узел не получает подтверждения того, что мастер-узел находится в сети, например если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (см. раздел « [Настройка шлюзов](#) »), и ни через один из шлюзов нет доступа в интернет.

Примечание Если проверка доступа в интернет настроена на каждом узле кластера и на всех узлах доступ в интернет отсутствует, перенос роли мастер-узла не выполняется, происходит прекращение обмена VRRP-сообщениями, и кластер отказоустойчивости приостанавливает работу.

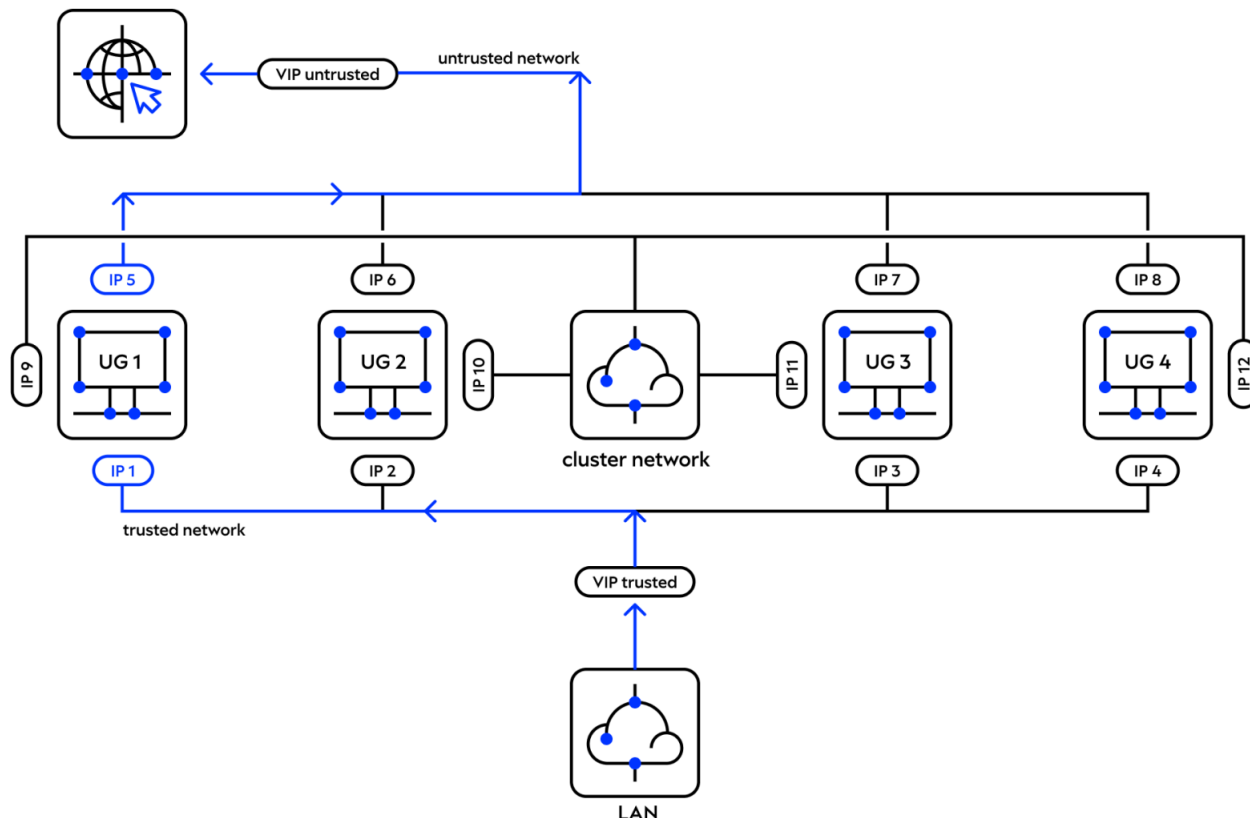
- Сбой в работе ПО UserGate WAF.

Примечание Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на резервный узел при переключении, устройству UserGate WAF посылается служебное оповещение GARP (Gratuitous ARP), извещающее сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. Пакет GARP отсылается UserGate WAF каждую минуту, в том числе при переключении роли мастер-узла на резервный узел.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме «активный — пассивный». Интерфейсы настроены следующим образом:

- Зона Trusted: IP1, IP2, IP3, IP4 и виртуальный cluster IP (VIP trusted).
- Зона Untrusted: IP5, IP6, IP7, IP8 и виртуальный cluster IP (VIP untrusted).
- Зона Cluster: IP9, IP10, IP11, IP12. Интерфейсы в зоне Cluster являются кластерными и используются для передачи VRRP-объявлений.

Оба виртуальных 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 на UG2.



Настройка кластера отказоустойчивости

Настройка кластера отказоустойчивости доступна только для узлов, входящих в кластер конфигурации.

Чтобы настроить кластер отказоустойчивости:

1. В разделе **Настройки → Сеть → Зоны** выберите зону, в которой планируется добавлять кластерные интерфейсы (зона Cluster на рисунках выше), и в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешите сервис **VRRP**.
2. В разделе **Настройки → Сеть → Интерфейсы** для каждого узла настройте интерфейсы для обмена VRRP-объявлениями между узлами кластера:
 - Выберите сетевой интерфейс, который будет участвовать в организации кластера.
 - В окне **Свойства интерфейса** на вкладке **Общие** установите флажок **Включено** и назначьте интерфейсу кластерную зону.
 - На вкладке **Сеть** добавьте IP-адрес, если он еще не был добавлен.

3. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** нажмите **Добавить**.
4. В окне **Свойства кластера отказоустойчивости** на вкладке **Общие** установите флажок **Включено** и введите название кластера.
5. На вкладке **Узлы** в блоке **Доступные узлы** выберите от двух до четырех узлов, затем в блоке **Настройка кластера** назначьте одному из узлов роль мастер-узла.

Примечание Если вы установите флажок «Не учитывать приоритет при смене роли мастер-узла», понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя.

6. На вкладке **Виртуальные IP-адреса** нажмите **Добавить** и назначьте интерфейсам узлов кластера, не участвующим в организации кластера и находящимся в одной зоне, общий виртуальный IP-адрес, на который будет направляться трафик. (На рисунках выше это один виртуальный IP-адрес для интерфейсов в зоне Trusted и еще один для интерфейсов в зоне Untrusted.)
7. Если необходимо, на вкладке **Общие** в блоке **Режим отправки служебного трафика** выберите режим обмена служебным трафиком между узлами кластера.
8. Если необходимо, настройте остальные параметры (см. таблицу ниже).
8. Сохраните изменения. В созданном кластере отказоустойчивости одному из узлов будет назначена роль мастер-узла, а на его сетевой интерфейс будет назначен указанный виртуальный IP-адрес.

В таблице описаны дополнительные параметры кластера отказоустойчивости.

Параметр	Описание

Параметр	Описание
Вкладка Общие	
Описание	Описание кластера отказоустойчивости
Идентификатор виртуального маршрутизатора (VRID)	Идентификатор, уникальный для каждого VRRP-кластера в локальной сети. Если в сети нет сторонних VRRP-кластеров, рекомендуется оставить значение по умолчанию
Режим отправки служебного трафика	Выбор режима обмена служебным трафиком между узлами кластера: • Мультикаст — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации. Вы можете выбрать другие интерфейсы. • Юникаст — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно после выбора узлов кластера на вкладке Узлы
Интервалы отправки и задержки	Параметры переключения роли мастер-узла на резервный узел: • Периодичность VRRP-объявлений — интервал в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. • Счетчик недоступности — количество интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. • Задержка смены роли по приоритету — время, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Эта задержка предоставляет время для сбора информации (например, о маршрутах) и позволяет избежать сбоя в работе сразу после переключения роли мастер-узла
Использовать виртуальный MAC	Если флажок установлен и на соответствующей вкладке параметров кластера отказоустойчивости назначены виртуальные IP-адреса, узлу с ролью мастер-узла назначается виртуальный MAC-адрес кластера. После этого в разделе Настройки → Сеть → Интерфейсы отобразится интерфейс VMAC. В случае переноса мастер-роли на резервный узел этот MAC-адрес сохраняется, что позволяет избежать задержек в передаче трафика
Разрешить транзит трафика через пассивные узлы	Если флажок установлен, резервный узел будет обрабатывать транзитный трафик, который поступает на его интерфейсы. В целях безопасности вы можете запретить обработку этого трафика, при снятом флажке он будет отбрасываться

Диагностика узлов кластера отказоустойчивости

Доступность узлов кластера определяется в том числе исходя из результатов диагностики состояния узлов. По умолчанию выполняется проверка состояния узлов кластера, локального DNS-сервера, прокси-сервера и кластерных интерфейсов узлов. Дополнительно вы можете например включить диагностику шлюзов или проверку доступа к сервисам, развернутым в ИТ-инфраструктуре, через узлы кластера.

Результаты диагностики влияют на условия переноса роли мастер-узла на резервный узел. По умолчанию перенос роли происходит без учета приоритета узлов. Например, при отключении одного из сетевых интерфейсов мастер-узла весь мастер-узел считается недоступным.

Вы можете настроить параметры таким образом, чтобы перенос роли мастер-узла зависел от понижения его приоритета при отключении одного или нескольких кластерных интерфейсов. Перенос роли мастер-узла на резервный узел произойдет, если приоритет последнего окажется выше приоритета мастер-узла. По умолчанию приоритет, назначенный мастер-узлу, равен 254, приоритет резервного узла — 253. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, который физически не подключен к сети. Соответственно, если на кластере отказоустойчивости, состоящем из двух узлов, один из интерфейсов на мастер-узле будет физически отключен от сети, резервный узел станет мастер-узлом (при условии, что на резервном узле все кластерные интерфейсы подключены к сети). В таком случае приоритет мастер-узла будет равен 252, приоритет резервного — 253. При восстановлении физического подключения на первоначальном мастер-узле этот узел снова станет мастер-узлом, поскольку его приоритет вернется в значение 254.

Примечание Отключение одного или нескольких кластерных интерфейсов на резервном узле также будет понижать его приоритет. Тем не менее этот резервный узел может стать мастер-узлом при безусловном переключении роли или в случае, если приоритет мастер-узла станет меньше приоритета резервного узла.

Чтобы настроить диагностику узлов кластера:

1. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** выберите кластер и нажмите **Редактировать**.

2. В окне **Свойства кластера отказоустойчивости** выберите вкладку **Диагностика**.

3. Установите флажок **Проверка шлюзов** и выберите, считать шлюз недоступным или понизить приоритет узла, если результаты проверки будут неудовлетворительными.

Примечание Чтобы помимо проверки самих шлюзов также выполнялась проверка доступа в интернет, необходимо включить проверку сети. Подробнее об этом — в разделе «[Настройка шлюзов](#)».

4. Настройте параметры проверки доступности шлюзов:

- **Периодичность запуска проверки** — регулярная проверка шлюзов через указанный промежуток времени.
- **Счетчик недоступности** — количество последовательных неудовлетворительных результатов проверки, после которых шлюз признается недоступным или приоритет узла понижается.
- **Счетчик доступности** — количество последовательных положительных результатов проверки, подтверждающее, что работоспособность шлюза восстановлена и узел можно признать доступным или повысить его приоритет.

5. Установите флажок **Проверка ресурсов** и выберите, считать узел недоступным или понизить приоритет узла, если проверка покажет, что указанные сервисы, развернутые в ИТ-инфраструктуре, недоступны.

6. Нажмите **Проверяемые ресурсы** и укажите IP-адреса или FQDN тех ресурсов, доступ к которым будет проверяться.

7. Настройте параметры проверки доступности ресурсов:

- **Периодичность запуска проверки** — регулярная проверка ресурсов через указанный промежуток времени.
- **Счетчик недоступности** — количество последовательных результатов проверки, после которых узел признается недоступным или его приоритет понижается.
- **Счетчик доступности** — количество последовательных положительных результатов проверки, подтверждающее, что доступ к ресурсу восстановлен и узел можно признать доступным или повысить его приоритет.

8. Установите флажок **Проверка интерфейсов**, нажмите **Настройки** и настройте следующие параметры:

- Для каждого из кластерных интерфейсов выберите действие, которое будет применено к узлу в случае недоступности интерфейса.
- Если необходимо отслеживать состояние сетевых интерфейсов, на которые назначены виртуальные IP-адреса, нажмите **Добавить**, выберите соответствующие сетевые интерфейсы и действия для них в случае недоступности.

9. Сохраните изменения.

Настройка кластера отказоустойчивости в облачной среде

Вы можете настроить кластер отказоустойчивости UserGate WAF в сервисе Yandex Cloud. Кластер отказоустойчивости, развернутый в облаке, может включать в себя только два узла, работающих в режиме «активный — пассивный», и поддерживает обмен служебными VRRP-объявлениями в юникаст-режиме.

Работа кластера отказоустойчивости в облачной среде возможна при соблюдении всех следующих условий:

- В кластере только два узла.
- Обмен служебным трафиком между узлами кластера выполняется в юникаст-режиме.
- Отключено использование виртуального MAC-адреса.
- Интерфейсам узлов кластера не назначены виртуальные IP-адреса.
- Отключена синхронизация пользовательских сессий.
- Маршрутизация входящего трафика выполняется внешним балансировщиком.
- Обеспечен доступ к таблицам маршрутизации Yandex Cloud и к API для работы с виртуальным частным облаком.

Перед тем как настроить параметры работы кластера UserGate WAF, подготовьте виртуальные машины в облачной среде:

1. Создайте в Yandex Cloud сервисный аккаунт с ролью `vpc.privateAdmin`.
2. Разверните в Yandex Cloud две виртуальные машины UserGate WAF и объедините их в кластер конфигурации.

Примечание Сервис Yandex Cloud поддерживает развертывание виртуальных машин как в одной сетевой зоне, так и в разных. Подробнее об этом — в [справке сервиса](#).

3. В веб-интерфейсе сервиса Yandex Cloud в параметрах каждой виртуальной машины добавьте созданный сервисный аккаунт.

4. Создайте таблицу маршрутизации Yandex Cloud. Когда кластер отказоустойчивости будет настроен, UserGate WAF передаст в эту таблицу IP-адрес сетевого интерфейса мастер-узла, через который будет направляться трафик. В случае если мастер-узел выйдет из строя, в таблицу статической маршрутизации Yandex Cloud будет передан IP-адрес резервного узла, и трафик перенаправится на этот IP-адрес.

Чтобы настроить кластер отказоустойчивости в облачной среде:

1. В разделе **Настройки → Сеть → Зоны** выберите или создайте зону для кластера и в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешит сервис **VRRP**.
2. В разделе **Настройки → Сеть → Интерфейсы** для каждого узла настройте интерфейсы для обмена VRRP-объявлениями между

узлами кластера:

- Выберите сетевой интерфейс, который будет участвовать в организации кластера.
 - В окне **Свойства интерфейса** на вкладке **Общие** назначьте интерфейсу кластерную зону.
 - На вкладке **Сеть** добавьте IP-адрес, если он еще не был добавлен.
 - Убедитесь, что на вкладке **Общие** установлен флажок **Включено**.
3. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** нажмите **Добавить**.
4. В окне **Свойства кластера отказоустойчивости** на вкладке **Узлы** в блоке **Доступные узлы** выберите виртуальные машины, развернутые в Yandex Cloud, затем в блоке **Настройка кластера** назначьте одной из виртуальных машин роль мастер-узла.
5. Убедитесь, что на вкладке **Виртуальные IP-адреса** интерфейсам узлов кластера не назначены виртуальные IP-адреса.
6. На вкладке **Общие** установите флажок **Включено** и введите название кластера.
7. В качестве режима отправки служебного трафика выберите **Юникаст** и нажмите **Настройки**.
8. В окне **Настройка интерфейсов для юникаст-трафика** в блоке **Передача VRRP-объявлений** выберите интерфейсы, которые были настроены на шаге 2, укажите их IP-адреса и сохраните изменения.
9. Убедитесь, что на вкладке **Общие** снят флажок **Использовать виртуальный MAC**.
10. Убедитесь, что на вкладке **Синхронизация сессий** сняты флажки **Синхронизировать сессии**.
11. На вкладке **Настройка облака** выберите в качестве облачного провайдера **Yandex Cloud**.
12. В блоке **Переключение маршрута** нажмите **Добавить** и в окне **Свойства переключения маршрута** настройте параметры, в соответствии с которыми в таблицу статической маршрутизации будет передаваться IP-адрес мастер-узла:
- В поле **Таблица маршрутизации** укажите идентификатор созданной ранее таблицы статической маршрутизации Yandex Cloud.
 - В поле **Префикс назначения** укажите префикс маршрута по умолчанию для таблицы статической маршрутизации Yandex Cloud.
 - В поле **<имя_узла_кластера_1>** для первого узла кластера укажите IP-адрес интерфейса, через который доступна внутренняя сеть.
 - В поле **<имя_узла_кластера_2>** для второго узла кластера укажите IP-адрес интерфейса, через который доступна внутренняя сеть, и сохраните изменения параметров переключения маршрута.
13. Сохраните изменения.

После сохранения изменений в таблицу статической маршрутизации Yandex Cloud с указанным идентификатором будут переданы префикс назначения и IP-адрес того узла, которому на вкладке **Узлы** назначена роль мастер-узла. Трафик будет направлен на IP-адрес мастер-узла.

Особенности настройки кластера отказоустойчивости с узлами в разных зонах Yandex Cloud

В зависимости от топологии и других особенностей ИТ-инфраструктуры вы можете настроить кластер отказоустойчивости, в котором узлы UserGate WAF будут располагаться в разных зонах Yandex Cloud. В этом случае, помимо общей настройки кластера, для каждого из узлов необходимо указать статические маршруты до подсети, находящейся за узлом в другой зоне. В противном случае активный узел кластера не сможет передавать ответы на запросы, поступающие из подсети в другой зоне.

Для каждого узла кластера выполните следующие действия:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** нажмите **Добавить**.
2. В раскрывающемся списке выберите **Статические маршруты** и нажмите **Добавить**.
3. В окне **Свойства маршрута** укажите его название, установите флажок **Включено**.
4. Убедитесь, что установлен тип маршрута **Unicast**.
5. В поле **Адрес назначения** укажите подсеть за другим узлом кластера, на которую будет указывать маршрут.
6. Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с узла, для которого настраивается маршрут.
7. Выберите сетевой интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, UserGate WAF сам определит интерфейс, исходя из параметров IP-адресации сетевых интерфейсов.
8. Сохраните изменения.

Просмотр информации о кластере отказоустойчивости

Вся информация о кластере доступна на странице **Кластеры отказоустойчивости**. Вы можете отслеживать состояние кластера отказоустойчивости и узлов, входящих в него. Также в веб-консоли выбранного узла на этой странице вы можете временно вывести этот узел из кластера, например для планового обслуживания. Для этого в блоке **Узлы** необходимо включить **Приостановить работу**.

Статусы кластера отказоустойчивости:

- Зеленый: кластер доступен.

- Оранжевый: неопределенное состояние кластера, как минимум один узел не участвует в работе кластера.
- Желтый треугольник: нет связи как минимум с одним узлом кластера, узел перезагружается или вышел из строя.

Статусы узлов в кластере отказоустойчивости:

- Зеленый: узел кластера доступен.
- Оранжевый: узел работоспособен, но недоступен в кластере.
- Желтый треугольник: узел перезагружается или вышел из строя.

