UserGate Management Center 6

Руководство администратора

Оглавление

1 ПРИНЯТЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение	Значение
UGMC	UserGate Management Center
МЭ	Межсетевой экран UserGate
ПАК	Программно-аппаратный комплекс
SU	Модуль лицензирования Security Update
УО	Управляемая область
УУ	Управляемое устройство МЭ UserGate
ПО	Программное обеспечение
ЦП	Центральный процессор

2 ВВЕДЕНИЕ

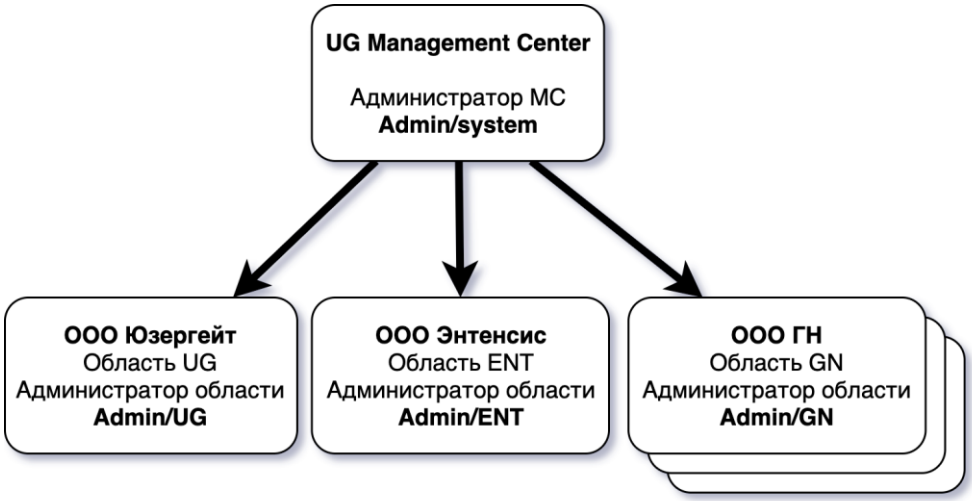
UserGate Management Center (UGMC) - это вспомогательный компонент для универсального межсетевого экрана UserGate (МЭ UserGate, МЭ), который позволяет управлять большим количеством устройств. UGMC предоставляет единую точку управления, из которой администратор может выполнять мониторинг серверов UserGate, применять необходимые настройки, создавать политики, применяемые к группам устройств для обеспечения безопасности корпоративной сети. Использование UGMC позволяет улучшить эффективность управления и поддержки распределенного парка межсетевых экранов UserGate.

UGMC поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде.

2.1 Управляемые области

UGMC поддерживает облачную модель управления, то есть предоставляет возможность полностью независимого управления МЭ разных предприятий, используя единый сервер управления. Разделение полномочий происходит на уровне управляемых областей. Управляемая область UserGate - это логический объект, представляющий одно предприятие или группу предприятий, управляемых одним администратором. Каждой области назначается отдельный администратор, который может администрировать только одну назначенную ему область. Администратор одной области не может ни при каких обстоятельствах получить доступ к другой области. Администратор сервера UGMC имеет полномочия создавать управляемые области и назначать в них администраторов, не имея при этом доступа к объектам самой области. Более подробно о разграничении прав администраторов смотрите в главе Администраторы.

Пример UGMC с несколькими управляемыми областями:



Для управления МЭ UserGate одной организации достаточно создать одну управляемую область.

Настройки параметров МЭ UserGate производятся внутри управляемой области с помощью шаблонов и групп шаблонов.

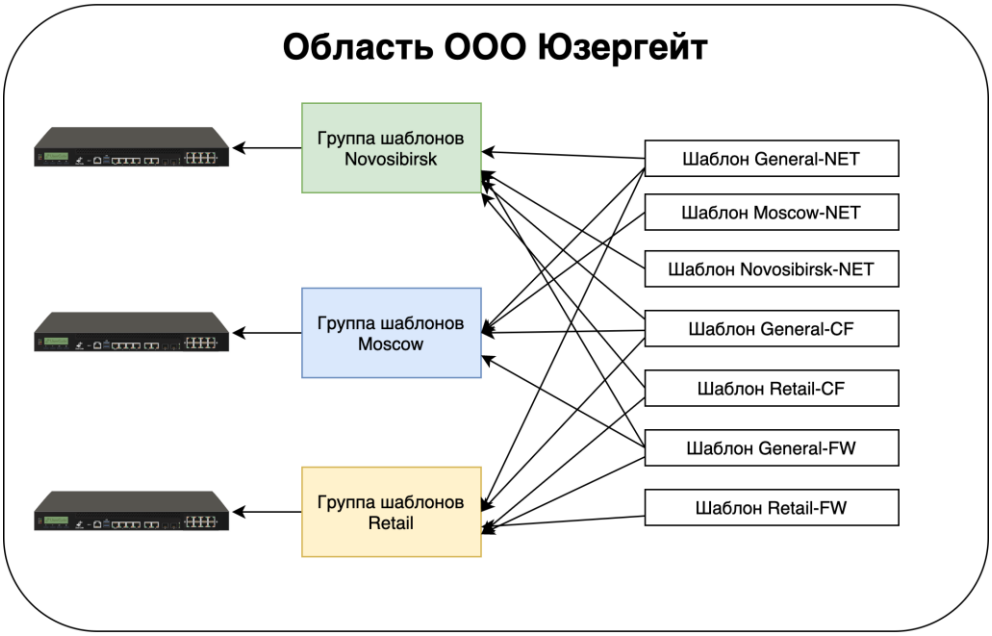
2.2 Шаблоны и группы шаблонов

С помощью шаблонов и групп шаблонов администратор управляемой области настраивает МЭ. Шаблон - это базовый блок, с помощью которого настраиваются все параметры работы межсетевого экрана -

сетевые настройки, правила межсетевого экрана, контентной фильтрации, системы обнаружения вторжений и других.

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Группы упрощают централизованное управление, поскольку позволяют задать базовую конфигурацию для всех МЭ с помощью одного или нескольких шаблонов, входящих в группу, оставив при этом возможность специфичной настройки каждого МЭ UserGate и добавляя специфичные настройки отдельными шаблонами. Результирующие настройки, применяемые к устройству МЭ, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы. Это позволяет определить группы шаблонов на основе функции географического расположения МЭ (например, Москва, Екатеринбург, Новосибирск и т. п.) или функциональной принадлежности МЭ (например, офис продаж, офис разработки, производство и т. п.).

Пример области с несколькими группами шаблонов:



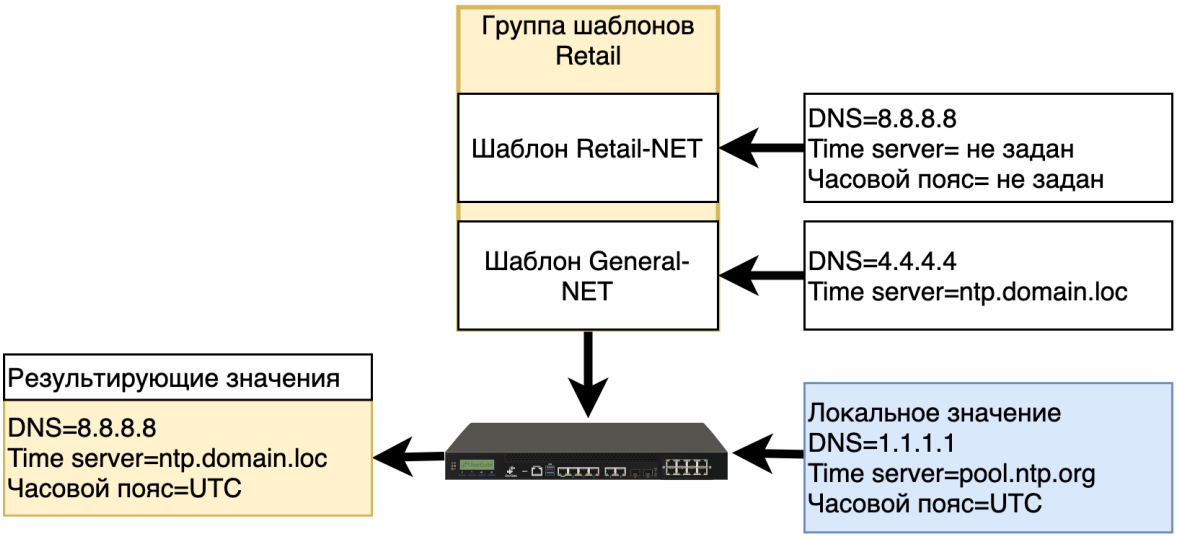
Конфигурация, передаваемая на устройство, может быть двух типов:

- Настройка параметра, например, IP-адрес сервера DNS.
- Правило политики, например, правило межсетевого экрана или контентной фильтрации.

Тип конфигурации определяет способ определения результирующего значения. Правила политики всегда передаются на все устройства, результирующая политика - это набор всех правил, выстроенных в соответствии с их порядком в групповом шаблоне. Правила, указанные в более верхнем шаблоне, помещаются вверх в результирующем списке правил на конечном устройстве.

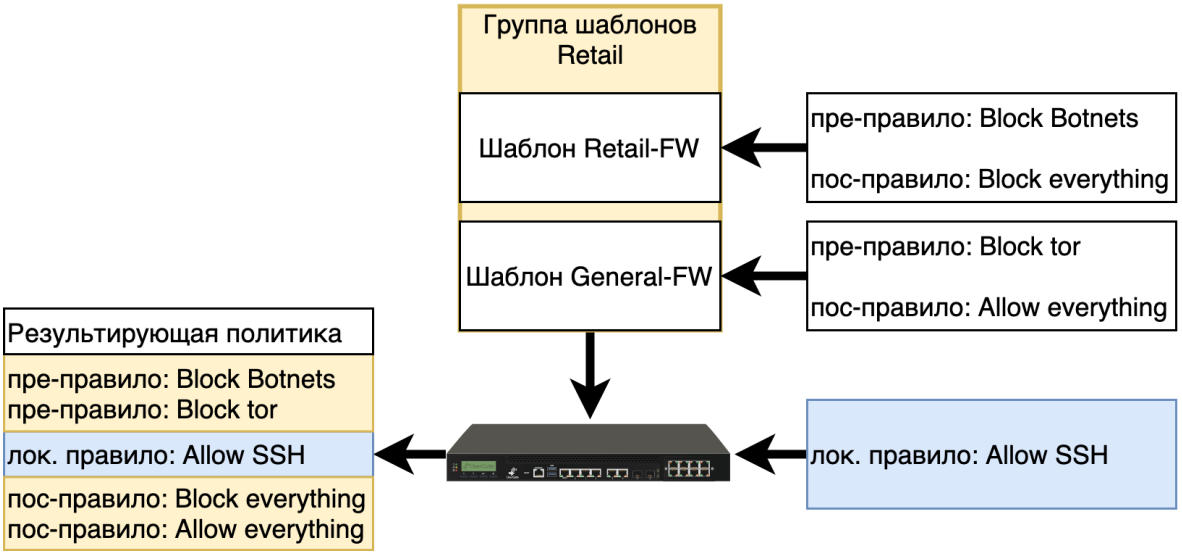
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

Пример результирующего значения параметра, определенного в нескольких шаблонах:



Правила, создаваемые в шаблонах, могут быть созданы как пре-правила или пост-правила. Пре- и пост-правила - это местоположение созданного правила относительно правил, создаваемых локальным администратором МЭ UserGate. Пре-правила всегда помещаются выше в списке правил и, следовательно, имеют более высокий приоритет относительно локально созданных правил. Пост-правила всегда помещаются ниже относительно локальных правил и имеют более низкий приоритет. Наличие возможности создавать пре- и пост-правила дает администратору области создавать гибкие настройки политики безопасности, давая локальному администратору больше полномочий (пост-правила), или ограничивая его полномочия (пре-правила).

Пример результирующей политики при наличии пре-, пост- и локальных правил:



2.3 Управляемые устройства

Группа шаблонов всегда применяется к одному или нескольким МЭ UserGate. МЭ UserGate является конечным управляемым устройством (УУ) в терминологии UserGate Management Center.

2.4 Управление UserGate Management Center

Управление UGMC делится на управление сервисами самой консоли и управление областями, которые в ней созданы.

2.4.1 Управление сервисами UGMC

Управление сервисами UGMC включает в себя следующие задачи:

Наименование	Описание
Настройка UGMC	• Назначение IP-адресов. • Конфигурирование зон. • Задание DNS-серверов. • Создание подключений к серверам LDAP. • Настройка оповещений. • Создание дополнительных администраторов UGMC с необходимым уровнем полномочий. Все эти настройки влияют только на функционирование самого сервиса UGMC и не влияют на администрирование управляемых областей.
Лицензирование	Лицензирование продукта (ввод ПИН-кода и регистрация продукта), а также опциональное назначение количества управляемых устройств каждой управляемой области. Если ограничения на область не установлены, то любая область может использовать любое количество управляемых устройств, в сумме не превышающих лицензируемое количество. Подробнее о лицензировании смотрите в главе Лицензирование UserGate Management Center.
Создание управляемых областей	Создание управляемых областей. Количество управляемых областей не ограничено.
Создание корневых администраторов управляемых областей	Создание корневых администраторов управляемых областей.

2.4.2 Управление областями UGMC

Управление областями выполняется администратором области и включает в себя следующие задачи:

Наименование	Описание
Создание дополнительных администраторов области	При добавлении управляемой области для неё создается корневой администратор, обладающий всеми полномочиями для управления данной областью. Корневой администратор области может создать дополнительных администраторов и наделить их необходимым уровнем полномочий.
Настройка серверов аутентификации	Создание подключений к серверам LDAP для возможности использования пользователей LDAP в качестве администраторов области.

Создание шаблонов устройств	Создание и настройка шаблонов устройств.
Создание групп шаблонов	Создание групп шаблонов, объединяющих в себя созданные ранее шаблоны.
Добавление управляемых устройств	Добавление управляемых устройств в UGMC и назначение им групп шаблонов.

2.4.3 Ролевое управление

При первоначальной настройке UGMC и создании хотя бы одной управляемой области создаются следующие администраторы:

- **Администратор UGMC.** Как правило это пользователь с именем Admin. Для входа в консоль необходимо указать имя в виде Admin/system; system означает, что вход осуществляется для управления сервисами UGMC, а не управляемой областью.
- **Корневой администратор созданной области**. Имя пользователя может быть любым, например, Admin. Для входа в консоль необходимо указать имя в виде Admin/realm_code, где realm_code - это код управляемой области.

Администратор UGMC может создать дополнительных администраторов UGMC и наделить их специальными полномочиями (профили администраторов) по управлению сервисами UGMC. При этом администраторы UGMC ограничены только возможностью управления сервисами UGMC (смотрите главу Настройка UserGate Management Center), не имея доступа к управлению областями. Пример прав доступа администраторов UGMC:

Администратор	Профиль администратора	Уровень доступа
Admin/system	Корневой профиль	Полный. Администратор и его профиль создаются при инициализации сервисов UGMC.
AdminRO/system	ReadOnly	Доступ ко всем сервисам UGMC в режиме просмотра без возможности модификации.
AdminRealm/system	RO+realms	Только создание управляемых областей и их администраторов и просмотр без модификации всех остальных настроек UGMC.
AdminDash/system	Dashboard	Только просмотр показаний раздела **Дашборд**.

Корневой администратор области может создать дополнительных администраторов в своей области и наделить их специальными полномочиями (профили администраторов). Администраторы области ограничены только возможностью управления своей областью (смотрите главу Управляемые области), не имея доступа к управлению другими областями или сервисами UGMC. Корневой администратор области может быть только локальным, он не может быть администратором, привязанным к каталогу LDAP. Дополнительные администраторы, созданные корневым администратором области, могут иметь тип

локального администратора или администратора, привязанного к каталогу LDAP. Примеры прав доступа администраторов области:

Администратор	Профиль администратора	Уровень доступа
Admin/realm_code	Корневой профиль	Полный. Администратор и его профиль создаются администратором UGMC.
AdminRO/realm_code	ReadOnly	Доступ ко всем настройкам области в режиме просмотра без возможности модификации.
AdminTemplates/realm_code	Templates	Создание и модификация всех шаблонов области.
AdminTemplateGeneral/realm_code	TemplateGeneral	Только модификация шаблона General.
AdminTemplateGeneralNET/realm_code	TemplateGeneralNET	Только модификация сетевых настроек в шаблоне General.

3 ЛИЦЕНЗИРОВАНИЕ USERGATE MANAGEMENT CENTER

UserGate Management Center лицензируется по количеству активных управляемых МЭ UserGate. При достижении максимального количества МЭ в UGMC, добавление нового МЭ станет невозможным. Учитываются только активные МЭ, которые включены в разделе **Управляемые устройства**. При наличии нескольких управляемых областей администратор может выделить необходимое количество лицензируемых устройств на каждую область. Общее количество управляемых устройств во всех областях ограничено только лицензией не может превышать количество лицензируемых устройств.

Лицензия на UGMC дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение: • Обновлений ПО UGMC. • Обновлений сигнатур системы обнаружения вторжений. • Обновление сигнатур приложений L7. • Технической поддержки. Модуль выписывается на 1 год, по истечении данного срока для получения обновлений и технической поддержки необходимо продление лицензии.

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Перейти в Дашборд	Находясь в разделе администрирования консоли нажать на пиктограмму **Дашборд** в правом верхнем углу.
Шаг 2. В разделе **Информация о лицензии** зарегистрировать продукт	В разделе **Информация о лицензии** нажать на ссылку **Зарегистрированная версия**, ввести ПИН-код и заполнить регистрационную форму.

Посмотреть статус установленной лицензии можно, находясь в разделе администрирования консоли в разделе **Дашборд** в виджете **Лицензия**.

4 ПЛАНИРОВАНИЕ ВНЕДРЕНИЯ USERGATE MANAGEMENT CENTER

Развертывание UGMC на предприятии требует тщательного планирования. От того, насколько качественно продумана архитектура шаблонов и групп шаблонов, зависит простота и гибкость применения политик управления на МЭ UserGate. UGMC позволяет эффективно применять общие политики, группируя их по географическому, функциональному или смешанному принципам.

При планировании архитектуры рекомендуется:

- Избегать конфликта настроек при добавлении шаблонов в группы шаблонов. Наличие конфликтов всегда усложняет управление конечными УУ. Это основополагающий принцип, из которого вытекают следующие рекомендации.
- Разделять различные группы настроек в разные шаблоны, например, общие настройки УУ в одном, политики контентной фильтрации в другом, политики межсетевого экранирования в третьем, политики СОВ в четвертом и так далее. Разнесение блоков настроек по разным шаблонам позволит избежать конфликта настроек и сделает централизованное управление проще.
- Создавать глобальные настройки в одних шаблонах, а необходимые для некоторых устройств специфические настройки - в других. Например, создать шаблон с правилами контентной фильтрации, применяемый для всех УУ, и еще один шаблон с правилами контентной фильтрации, применяемый только для группы устройств. Варьируя положение этих двух шаблонов в группах устройств, администратор может выстроить правильный порядок результирующих правил на конечных устройствах. Данная рекомендация допускает контролируемое количество конфликтных настроек.
- Помнить про полномочия локальных администраторов. Если предполагается наличие локальных администраторов, то их полномочия будут ограничены настройками тех параметров, которые не заданы через шаблоны UGMC, а правила, созданные локальными администраторами, всегда помещаются между пре- и пост- правилами, применяемыми из UGMC.

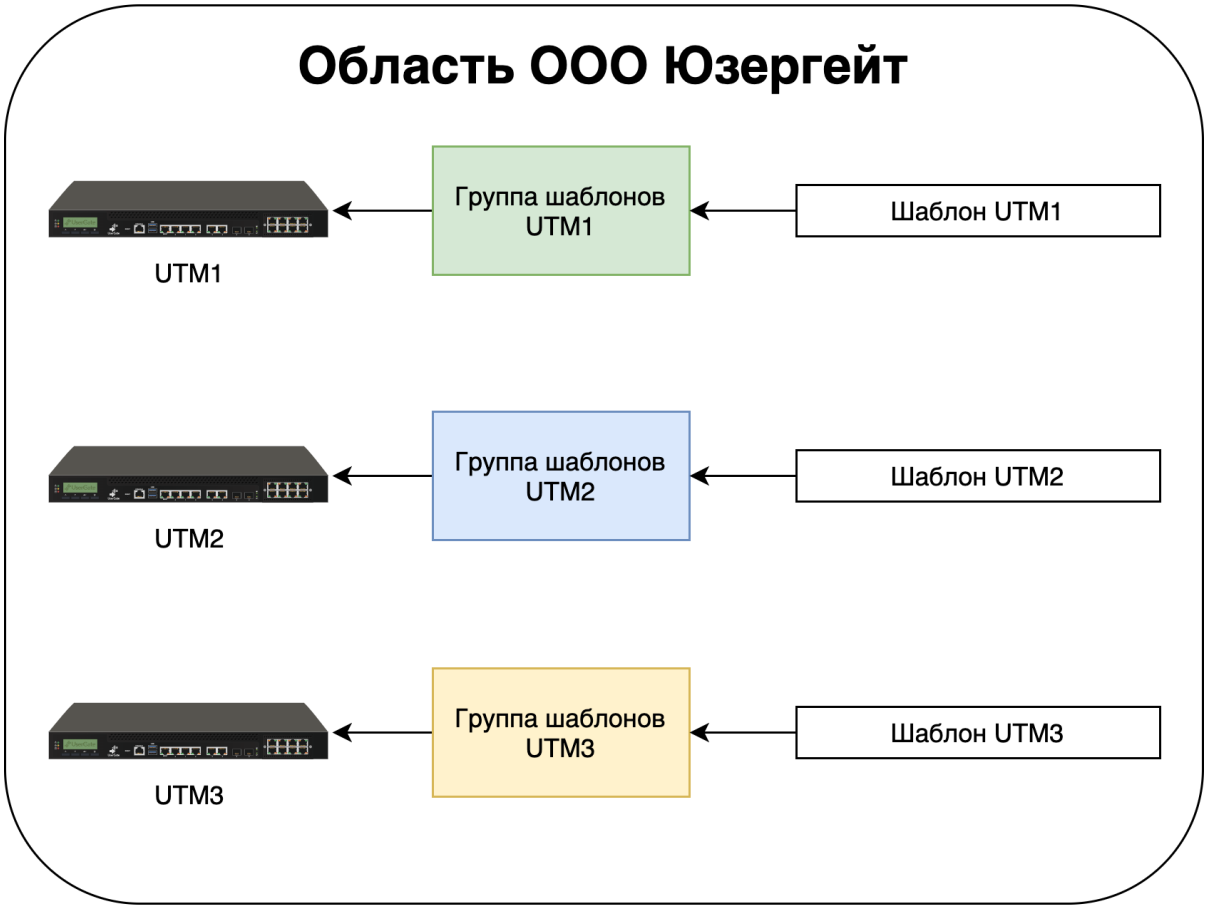
Для вывода устройств из-под управления UserGate Management Center необходимо отменить применение всех шаблонов с настройками (например, создать пустую группу шаблонов и назначить её управляемому устройству) и выполнить синхронизацию управляемого устройства и UGMC.

Рассмотрим несколько типичных сценариев внедрения UGMC.

4.1 Один шаблон и одна группа шаблонов на каждое управляемое устройство

Самый простой вариант развертывания UGMC. К его преимуществам следует отнести простоту и прозрачность настроек, к недостаткам - отсутствие централизованного применения политик - для каждого из устройств придется настраивать свою собственную политику. Настройки сетевых подключений могут производиться как через шаблоны UGMC, так и локальным администратором.

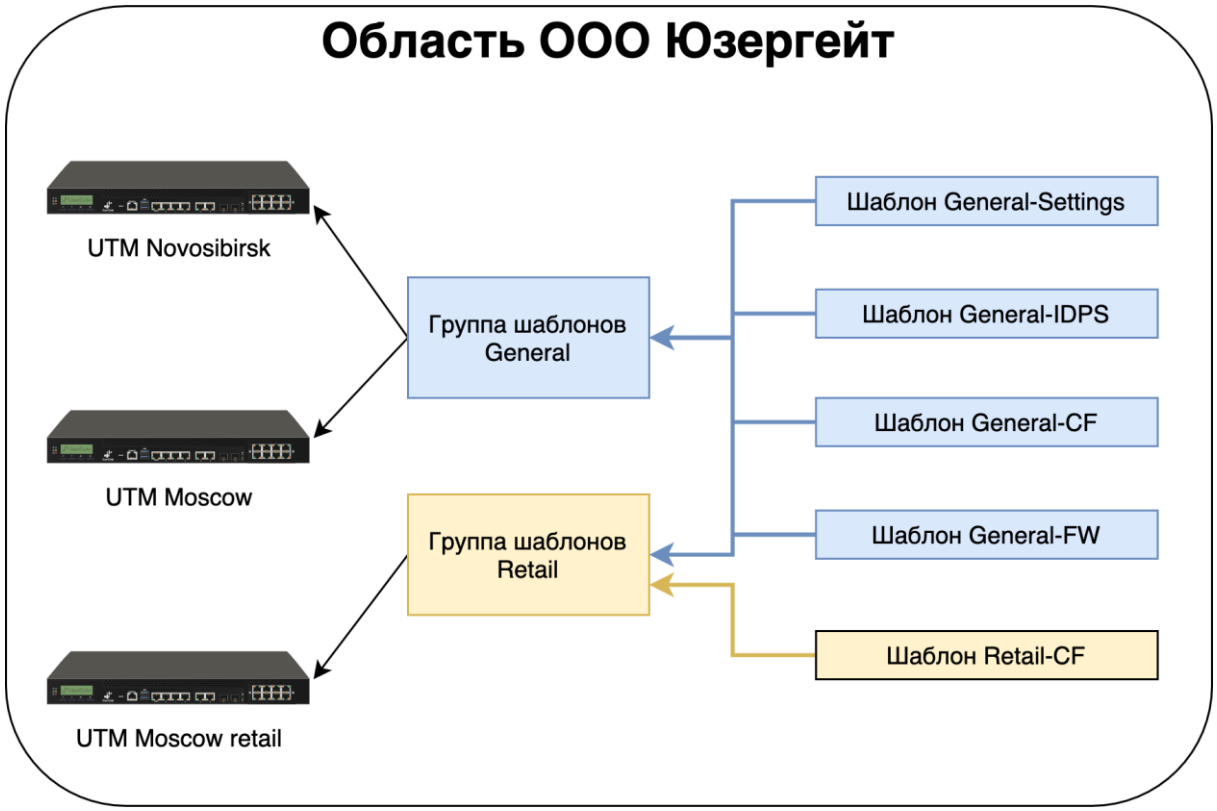
Рекомендуется для простых внедрений с небольшим количеством МЭ UserGate. Пример такой настройки представлен на рисунке ниже.



4.2 Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы УУ. Сеть настраивается локально

Настройки разбиты по шаблонам, каждый из которых отвечает за настройки специфического модуля, что позволяет избежать конфликта настроек. Суммарно все шаблоны формируют центрально управляемую политику, применяемую ко всем УУ в компании. Для специфических УУ, которым необходима специальная политика, добавляются отдельные шаблоны. Сетевые интерфейсы настраиваются локальными администраторами.

Рекомендуется для большинства предприятий. Пример такой настройки представлен на рисунке ниже.



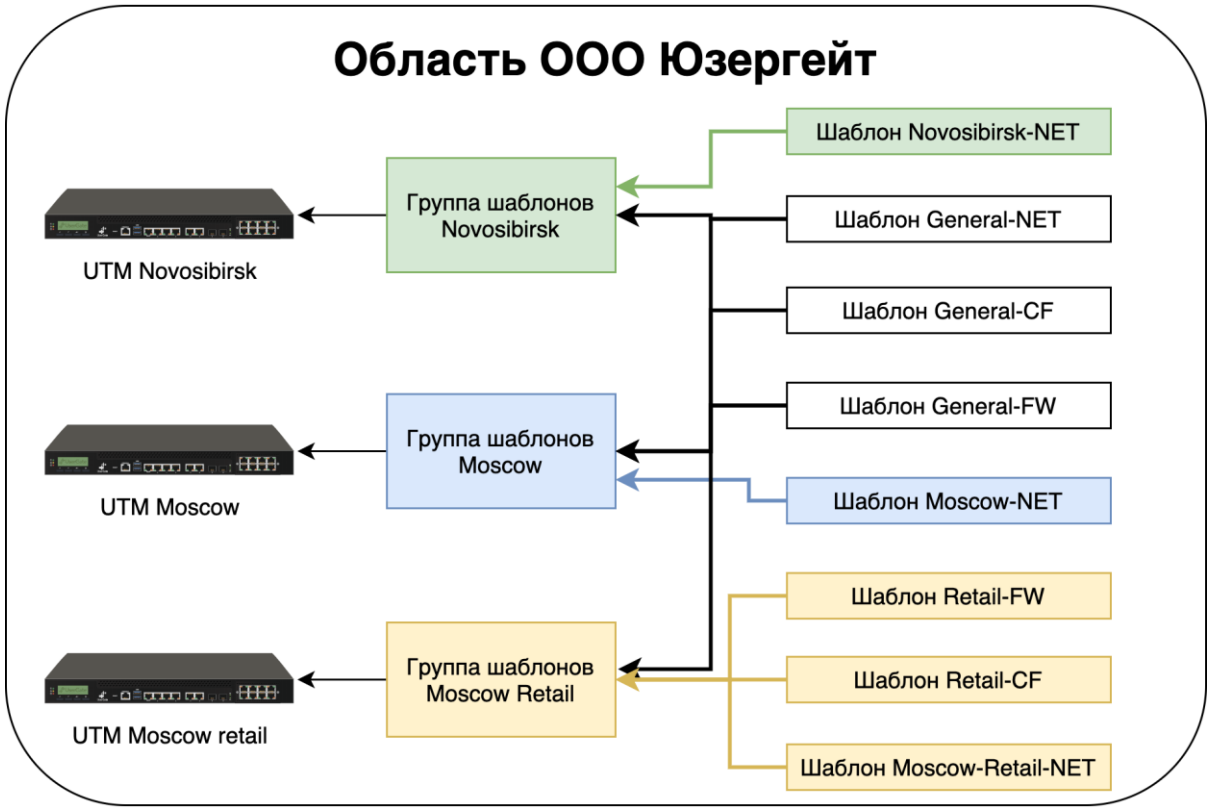
В данном примере шаблоны содержат следующие настройки:

- Шаблон General-Settings - общие для всех настройки (time zone, уровень журналирования, сервера DNS, и т.п.).
- Шаблон General-IDPS - общие для всех политики системы обнаружения вторжений.
- Шаблон General-CF - общие для всех политики контентной фильтрации.
- Шаблон General-FW - общие для всех политики межсетевого экранирования.
- Шаблон Retail-CF - специфичные для ритейловых подразделений политики контентной фильтрации.

4.3 Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы УУ. Сеть настраивается через UGMC

Аналогично предыдущему варианту, но с дополнительным шаблоном сетевых настроек для каждого из МЭ UserGate.

Рекомендуется для большинства предприятий, где необходима централизованная настройка сетевых интерфейсов. Пример такой настройки представлен на рисунке ниже.



В данном примере шаблоны содержат следующие настройки:

- Шаблон General-NET - общие для всех настройки сетевых портов.
- Шаблон General-CF - общие для всех политики контентной фильтрации.
- Шаблон General-FW - общие для всех политики межсетевого экранирования.
- Шаблон Retail-CF - специфичные для ритейловых подразделений политики контентной фильтрации.
- Шаблон Novosibirsk-NET - специфичные для Новосибирского подразделения настройки сетевых портов.
- Шаблон Moscow-NET - специфичные для Московского подразделения настройки сетевых портов.
- Шаблон Moscow-Retail-NET - специфичные для Московского ритейл подразделения настройки сетевых портов.

4.4 Примеры шаблонов устройств

UserGate Management Center поставляется с созданной по умолчанию областью (Example realm), которая содержит в себе шаблоны NGFW.

Примечание

Область и представленные в ней шаблоны созданы исключительно для удобства пользователей. Элементы могут быть использованы или удалены за ненадобностью.

Для входа в область Example realm используйте созданный по умолчанию профиль администратора области с логином/паролем – ex_admin/Example.

В области представлены следующие шаблоны NGFW:

- **example_content_template**: примеры настройки правил контентной фильтрации.

- **example_firewall_template**: примеры настройки правил межсетевого экранирования.
- **example_settings**: общие настройки UserGate (часовой пояс, язык интерфейса, настройки времени сервера).
- **UserGate Libraries template**: набор зон и элементов библиотек: сервисы, календари, полосы пропускания, шаблоны страниц, категории URL, профили SSL.

Примечание

В случае удаления шаблона UserGate Libraries template все элементы, добавленные UserGate по умолчанию, станут недоступными для использования и будут удалены. Рекомендуется не удалять данный шаблон и при настройке политик, связанных с наборами этого шаблона, использовать сам шаблон или его копию.

5 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

UserGate Management Center поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины UserGate Management Center поставляется с двумя Ethernet-интерфейсами. В случае поставки в виде ПАК UserGate Management Center может содержать 8 или более Ethernet-портов.

5.1 Развертывание программно-аппаратного комплекса

В случае поставки решения в виде ПАК, программное обеспечение уже загружено и готово к первоначальной настройке. Перейдите к главе Подключение к UserGate Management Center для дальнейшей настройки.

5.2 Развертывание виртуального образа

UserGate Management Center Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры как VMWare, Oracle VirtualBox. Для Microsoft Hyper-v и KVM поставляются образы дисков виртуальной машины.

Примечание

Для корректной работы виртуальной машины рекомендуется использовать минимум 8 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Для начала работы с виртуальным образом, выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru.
Шаг 2. Импортируйте образ в свою систему виртуализации	Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины.
Шаг 3. Настройте параметры виртуальной машины	Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb.
Шаг 4. Важно! Увеличьте размер диска виртуальной машины	Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 300Gb или более. Рекомендованный размер - 500Gb или более.

Шаг 5. Настройте виртуальные сети	UserGate Management Center поставляется с двумя интерфейсами, назначенными в зоны: • Management - первый интерфейс виртуальной машины. • Trusted - второй интерфейс виртуальной машины, предназначенный для связи с управляемыми МЭ UserGate.
Шаг 6. Выполните сброс к заводским настройкам	Запустите виртуальную машину. Во время загрузки выберите **Support Tools** и выполните **Factory reset**. **Этот шаг крайне важен**. Во время этого шага UGMC настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до размера, указанного в 4-м пункте.

5.3 Подключение к UserGate Management Center

Интерфейс сервера port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе Интерфейс командной строки (CLI).

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления	**При наличии DHCP-сервера** Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить сервер UserGate Management Center. После загрузки консоль UserGate укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. **Статический IP-адрес** Включить сервер UGMC. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли UGMC по указанному адресу, он должен выглядеть примерно следующим образом: https://UserGate_MC_IP_address:8010
Шаг 2. Выбрать язык	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль корневого администратора UserGate Management Center	Задать логин и пароль для входа в веб-интерфейс управления.

Шаг 4. Зарегистрировать систему	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ UGMC в интернет. Если на данном этапе выполнить регистрацию не удается, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.
Шаг 5. Настроить зоны, IP-адреса интерфейсов, подключить UserGate Management Center в сеть предприятия	В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона **Management** (сеть управления), интерфейс port0. • Зона **Trusted** (LAN). Предполагается, что через эту зону UGMC будет подключаться к МЭ UserGate, а также получит доступ в интернет. Для работы UGMC достаточно одного настроенного интерфейса. Разделение функций управления устройством UGMC и управления МЭ UserGate на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.
Шаг 6. Настроить шлюз в интернет	В разделе **Шлюзы** указать IP-адрес шлюза в интернет на интерфейсе, который имеет доступ в интернет, как правило, это зона Trusted. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов.
Шаг 7. Указать системные DNS-серверы	В разделе **DNS** укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации.
Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4)	Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate Management Center.
Шаг 9. Создать как минимум одну управляемую область	В разделе **Управляемые области --> Области** добавить управляемую область.
Шаг 10. Создать администратора созданной управляемой области	В разделе **Администраторы** создать профиль администратора и дать ему права на управление созданной областью. Создать администратора с данным профилем.
Шаг 11. Создать дополнительных администраторов UGMC (опционально)	В разделе **Администраторы** создать необходимые профили для управления сервисами UGMC и создать администраторов UGMC с этими профилями.

После выполнения вышеперечисленных действий UserGate Management Center готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

6 НАСТРОЙКА USERGATE MANAGEMENT CENTER

В данном разделе руководства описываются настройки сервиса консоли UserGate. Настройка управляемых областей и применение политик безопасности к МЭ UserGate описано в главе данного руководства Управление областями UGMC.

6.1 Общие настройки

Раздел **Общие настройки** определяет базовые установки UserGate Management Center:

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.
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.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS.

6.2 Управление устройством

Раздел **Управление устройством** определяет следующие установки UGMC:

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

6.2.1 Кластеризация и отказоустойчивость

UGMC 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.

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 диагностики Настройки интерфейсов Настройки шлюзов Маршруты

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. 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.
Шаг 5. Подключить второй узел в кластер	Второй и последующие узлы подключаются в кластер на моменте первоначальной инициализации. Если инициализация уже была проведена, то необходимо перезагрузить устройство и выполнить возврат к заводским установкам (Factory reset) - смотрите разделе Офлайн операции с сервером. Подключитесь к веб-консоли второго узла кластера, выберите язык установки, часовой пояс, примите лицензионное соглашение и на следующем этапе выберите ссылку **Установка дополнительного узла кластера**.

	Укажите интерфейс, который будет использован для подключения к первому узлу кластера и назначьте 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. Укажите IP-адрес мастер узла, настроенный на шаге 3, вставить секретный код и нажмите на кнопку **Подключить**. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер, и все настройки первого узла кластера реплицируются на второй.
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 и другие настройки, индивидуальные для каждого из узлов.

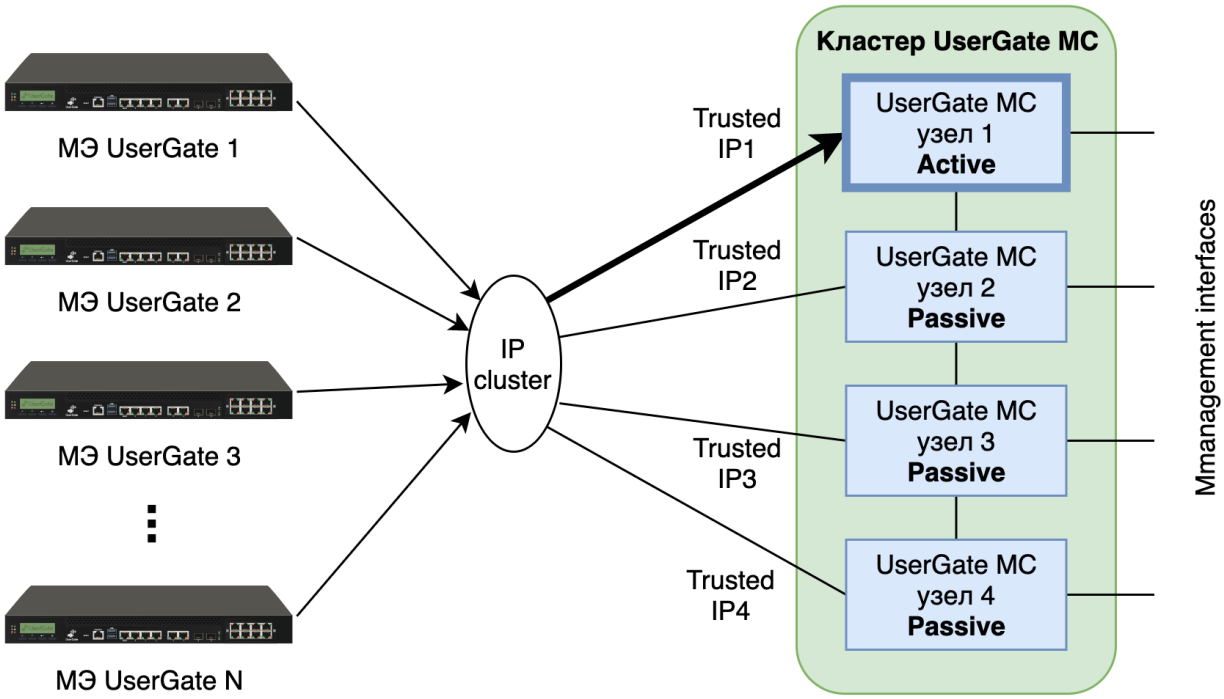
До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько. Поддерживаются 2 режима - **Актив-Актив** и **Актив-Пассив**.

В режиме **Актив-Пассив** один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные - в качестве резервных. Для кластера указывается один или более виртуальных IP-адресов. Переключение виртуальных адресов с главного на один из запасных узлов происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На главном узле настроена проверка доступа в интернет.
- Сбой в работе ПО UserGate.

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

- **Зона Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Management**: интерфейсы в зоне Management используются для управления узлами UGMC.



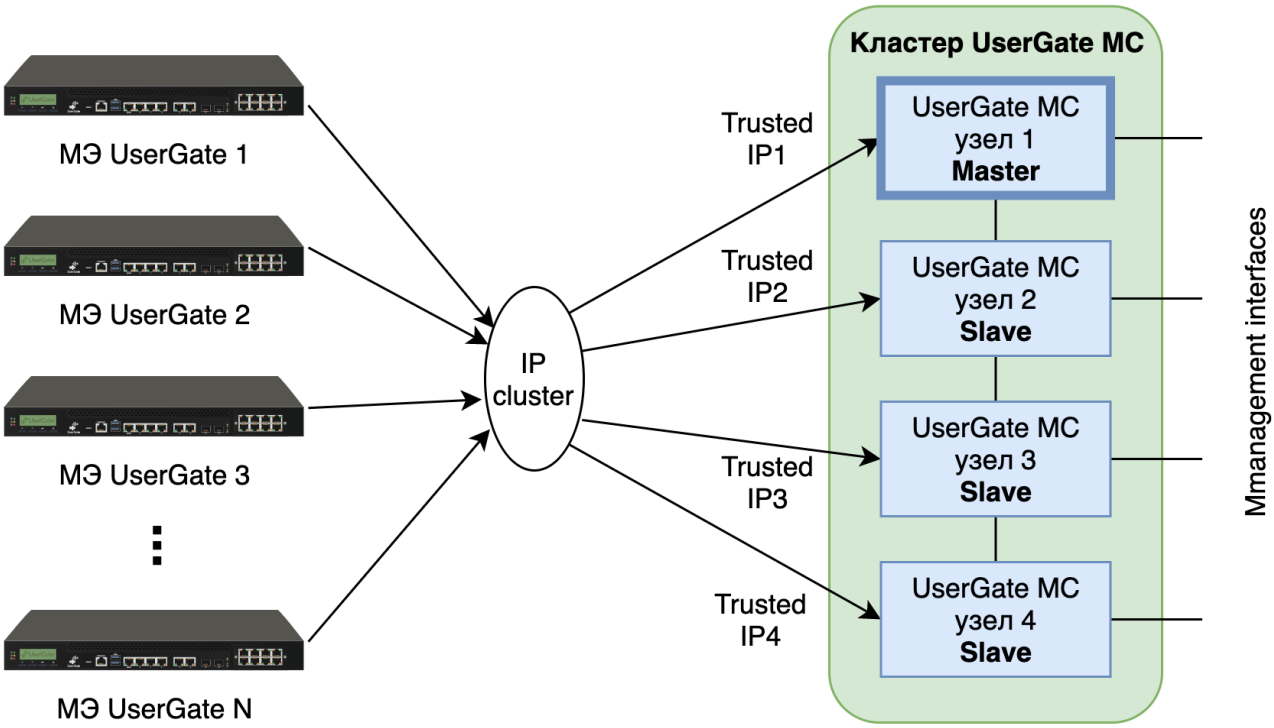
Кластерный IP-адрес находятся на узле UGMC 1. Если узел UGMC 1 становится недоступным, то кластерный IP-адрес перейдет на следующий сервер, который станет мастер-сервером, например, UGMC 2.

В режиме **Актив-Актив** один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера. Поскольку IP-адрес кластера находится на Мастер-узле, то Мастер-узел отвечает на ARP-запросы клиентов. Выдавая последовательно MAC-адреса всех узлов отказоустойчивого кластера, Мастер-узел обеспечивает равномерное распределение трафика на все узлы кластера, учитывая при этом необходимость неразрывности пользовательских сессий. Для кластера указывается один или более виртуальных IP-адресов. Перемещение роли Мастер-узла на один из запасных узлов происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На главном узле настроена проверка доступа в интернет.
- Сбой в работе ПО UserGate.

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 Management**: интерфейсы в зоне Management используются для управления узлами UGMC.



Кластерный IP-адрес находятся на узле UGMC 1, который является мастер-узлом. При этом трафик распределяется на все узлы кластера. Если узел UGMC 1 становится недоступным, то роль мастера и кластерный IP-адрес перейдет на следующий сервер, например, UGMC 2.

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 (зона **Trusted** на диаграммах выше).
Шаг 3. Создать кластер отказоустойчивости	В разделе **Управление устройством --> Кластер отказоустойчивости** нажать на кнопку **Добавить** и указать параметры кластера отказоустойчивости.

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.
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.

6.2.2 Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки UGMC 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 UGMC.
Журналы диагностики	• **Скачать журналы** - скачать диагностические журналы для передачи их в службу поддержки UserGate. • **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 UGMC для диагностики и решения проблем. Для успешной активации удаленного помощника UGMC должен иметь доступ к серверу удаленного помощника компании UserGate 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

6.2.3 Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

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

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UGMC в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе Лицензирование UserGate Management Center). При наличии обновлений в разделе **Управление устройством** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя UGMC.

Для установки обновлений необходимо выполнить следующие действия:

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

6.2.4 Экспорт настроек

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

Примечание

Экспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо настроить интерфейсы и повторно зарегистрировать UGMC с помощью имеющегося ПИН-кода.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе **Управление устройством** нажать на ссылку **Экспорт настроек --> Экспорт** и выбрать **Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит: • текущие настройки сервера под именем: cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin • сетевые настройки под именем: network-cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename – имя узла UserGate Management Center. version – версия UserGate Management Center. YYYYMMDD_HHMMSS – дата и время выгрузки настроек в часовом поясе UTC. Например, cc_core-mc_core@ediasaionedi_6.1.8.93R-1_20220715_084853.bin или network-cc_core-mc_core@ediasaionedi_6.1.8.93R-1_20220715_084929.bin.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе **Управление устройством** нажать на ссылку **Экспорт настроек --> 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 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:0-31) (месяц:0-12) (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.

6.3 Администраторы

Доступ к веб-консоли UGMC 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.

Примечание

При первоначальной настройке UGMC создается локальный суперпользователь Admin/system.

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 аутентификации**. При входе в консоль администрирования необходимо указывать имя пользователя

	в формате user@domain/system или domain\user/system. Назначить созданный ранее профиль. • **Добавить группу LDAP** - добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы аутентификации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain/system или domain\user/system. Назначить созданный ранее профиль. **Важно!** В данном разделе настроек сервисов консоли управления администратором области может быть назначен только локальный администратор. Это связано с тем, что LDAP серверы, используемые для аутентификации администраторов сервиса UGMC и для аутентификации администраторов области, могут быть разными. При необходимости использования LDAP администраторов для управления Областью, их необходимо создать в самой области. Более подробно об администраторах области смотрите в разделе Администраторы области.

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля
Описание	Описание профиля
Тип администратора	Для предоставления полномочий управления сервисами UGMC необходимо выбрать тип **Администратор UGMC**. Вариант **Администратор области** следует выбирать при создании корневого администратора управляемой области.
Управляемая область	Если в качестве параметра **Тип администратора** был выбран вариант **Администратор области**, то необходимо указать управляемую область, для которой создается корневой администратор. Область должна уже быть создана к этому моменту.
Права доступа	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа • Чтение • Чтение и запись

Администратор UGMC 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.

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

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8010).

Примечание

Не 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 во вкладке **Контроль доступа** разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе Настройка зон.

6.4 Управление сертификатами

UGMC использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции UGMC использует сертификат типа **SSL веб-консоли**.

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 UGMC. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку **Редактировать** и указать тип сертификата - SSL веб-консоли. После этого UGMC перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

UGMC 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.
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • **Экспорт сертификата** - экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. • **Экспорт CSR** - экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

Примечание

Рекомендуется сохранять сертификат для возможности его последующего восстановления.

Примечание

В целях безопасности UGMC 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. • Загрузите файл, содержащий данные сертификата. • 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.

6.5 Профили оповещений

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Аутентификация	Включает аутентификацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.

Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL – 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

6.6 Серверы аутентификации UserGate Management Center

Серверы аутентификации - это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UGMC. UGMC поддерживает только сервер аутентификации LDAP-коннектор. LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию администраторов UGMC через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.

SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена. Для входа в консоль пользователям LDAP необходимо указывать имя в формате:

domain\user/system или *user@domain/system*

7 ОФЛАЙН ОПЕРАЦИИ С СЕРВЕРОМ

Некоторые операции с сервером проводятся, когда сервер не выполняет свою функцию и находится в офлайн режиме. Для выполнения таких операций необходимо во время загрузки сервера выбрать раздел меню **Support menu** и затем одну из требуемых операций. 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 MC. 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 MC (serial console)	Загрузка UserGate MC с выводом диагностической информации о загрузке в последовательный порт.
2. UserGate MC (verbouse mode)	Загрузка UserGate MC 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.
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 MC. Данные и настройки UserGate MC не сбрасываются.

Backup full	Создать полную копию диска UserGate MC на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Backup system only	Создать копию системного раздела UserGate MC, исключая журналы на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate MC с внешнего USB носителя.
Update from USB	Установка обновления ПО UserGate MC 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 версии).
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 MC, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UserGate MC не сбрасываются.
Factory reset	Сброс состояния UserGate MC к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

8 НАСТРОЙКА СЕТИ

В данном разделе описаны сетевые настройки UserGate Management Center.

8.1 Настройка зон

Зона в UGMC - это логическое объединение сетевых интерфейсов. Политики безопасности UGMC используют зоны интерфейсов, а не непосредственно интерфейсы.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов управления.

По умолчанию UGMC поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление UGMC.
Trusted	Зона для подключения управляемых устройств и получения доступ в сеть интернет.

Для работы UGMC достаточно одного настроенного интерфейса. Разделение функций управления устройством и управления МЭ UserGate на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Администраторы UGMC могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.

Примечание

Можно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону	Нажать на кнопку **Добавить** и дать название зоне.
Шаг 2. Настроить параметры защиты зоны от DoS (опционально)	Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • **Порог уведомления** - при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал. • **Порог отбрасывания пакетов** - при превышении количества запросов с одного IP-адреса над указанным значением UGMC начинает отбрасывать пакеты, поступившие с этого IP-адреса, и записывает данное событие в системный журнал.

	Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов - 600 запросов в секунду. **Исключения защиты от DoS** - позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для шлюзов UserGate, которые могут слать большой объем данных на сервера UGMC.
Шаг 3. Настроить параметры контроля доступа зоны (опционально)	Указать предоставляемые UGMC сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы. Сервисы: • **Ping** – позволяет пинговать UGMC. • **Консоль администрирования** - доступ к веб-консоли управления (TCP 8010 и 8300). • **XML-RPC для управления** – позволяет управлять продуктом по API (TCP 4040). • **VRRP** – сервис, необходимый для объединения нескольких устройств UserGate в отказоустойчивый кластер (IP протокол 112). • **Кластер** – сервис, необходимый для объединения нескольких устройств UserGate в кластер (TCP 4369, TCP 9000-9100). • **CLI по SSH** – доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **Сервис UserGate Management Center** – сервис подключения МЭ UserGate (TCP 2022, 9712). Подробнее о требованиях сетевой доступности читайте в Приложение 1. Требования к сетевому окружению.
Шаг 4. Настроить параметры защиты от IP-спуфинг атак (опционально)	Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из **Trusted**, в другую, например, в **Management**. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес. Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников отличных от указанных будут отброшены. С помощью чекбокса **Инвертировать** администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0./16 и включить опцию **Инвертировать**.

8.2 Настройка интерфейсов

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN и бонд-интерфейсы.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.
- Указать тип интерфейса - Layer 3.

- Назначить зону интерфейсу.
- Изменить физические параметры интерфейса - MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.

8.2.1 Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Вкл	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • **Round robin**. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • **Active backup**. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • **XOR**. Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • **Broadcast**. Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • **IEEE 802.3ad** - режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику.

	• **Adaptive transmit load balancing**. Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • **Adaptive load balancing**. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию - 0 - отключает MII-мониторинг.
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • **Slow** - запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • **Fast** - запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • **Отключено** - устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • **Active** - MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • **Follow** - MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.

Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • **Layer 2** - использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • **Layer 2+3** - использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • **Layer 3+4** - используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

8.3 Настройка шлюзов

Для подключения UGMC к интернету необходимо указать IP-адрес одного или нескольких шлюзов.

Можно указать несколько шлюзов, если для подключения к интернету используется несколько провайдеров. Пример настройки сети с двумя провайдерами:

- Интерфейс port1 с IP-адресом 192.168.11.2 подключен к интернет-провайдеру 1. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1
- Интерфейс port2 с IP-адресом 192.168.12.2 подключен к интернет-провайдеру 2. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок **Балансировка** и указать **Вес** каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз).
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить **Проверку сети**, нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли.

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

8.4 Маршруты

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута	В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 2. Указать адрес назначения	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172 .16.20.5/32.
Шаг 3. Указать шлюз	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UGMC.
Шаг 4. Указать интерфейс	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UGMC сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

9 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI)

UGMC позволяет создавать базовые настройки устройства с помощью интерфейса командной строки, 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 UGMC), 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 UGMC	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 корневого администратора UGMC (по умолчанию Admin/system). Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, в качестве пароля - utm.

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

Наименование	Описание
Шаг 1. Подключиться к UserGate Management Center	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UGMC.
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 корневого администратора UGMC (по умолчанию Admin/system). Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, 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 UGMC, в качестве порта подключения - 2200, в качестве имени пользователя - имя пользователя правами корневого администратора UGMC (по умолчанию Admin/system). Для Linux команда на подключение должна выглядеть так: *ssh Admin/system@IPUserGateMC -p 2200*
Шаг 3. Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, 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.
date	Посмотреть текущее время на сервере.
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.
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.
nslookup	Выполнить определение IP-адреса по имени хоста.
ping	Выполнить ping определенного хоста.
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 UGMC завис.
reboot	Перезагрузить сервер UserGate Management Center.
route	Создать, изменить, удалить маршрут.
shutdown	Выключить сервер UGMC.
traceroute	Выполнить трассировку соединения до определенного хоста.
zone	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

10 УПРАВЛЕНИЕ ОБЛАСТЯМИ

Управляемая область UserGate - это логический объект, представляющий одно предприятие или группу предприятий, управляемых единым администратором или группой администраторов. Для управления МЭ UserGate корневой администратор UGMC (или администратор UGMC с соответствующими полномочиями) должен создать как минимум одну область.

10.1 Создание управляемых областей

Для создания управляемой области администратор UGMC должен выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать область	В разделе веб-консоли **Управляемые области --> Области** нажать кнопку **Добавить**, заполнить необходимые поля.
Шаг 2. Создать профиль администратора с типом администратор области	В разделе веб-консоли **Администраторы --> Профили администраторов** нажать кнопку **Добавить** и создать профиль администратора с типом администратор области и правом на созданную на предыдущем шаге область.
Шаг 3. Создать администратора области	В разделе веб-консоли **Администраторы --> Администраторы** нажать кнопку **Добавить** и создать администратора с созданным ранее профилем.

При создании области необходимо указать следующие поля:

Наименование	Описание
Область по умолчанию	Если данная галочка установлена, то при авторизации в веб-консоль необязательно указывать имя области через слэш.
Название	Название области, например, ООО Юзергейт.
Код области	Код из нескольких букв и/или цифр. Код области необходимо указывать при входе в веб-консоль для управления данной областью. Например, UG.
Описание	Опциональное описание области.
Количество устройств	Если указано, то администратор области будет ограничен этим количеством и не сможет создать большее количество управляемых устройств. Заданное количество не может превышать количество лицензированных подключений.

При создании профиля администратора необходимо указать тип администратора - администратор области и в качестве управляемой области указать созданную область. Для создания администратора области необходимо выбрать данный профиль администратора области. Подробнее о создании администраторов смотрите в главе данного руководства Администраторы.

После создания области и администратора данной области можно переключиться в режим управления данной областью. Для этого необходимо выйти из-под учетной записи администратора UGMC в веб-консоли и заново зайти под учетной записью администратора управляемой области. Имя администратора следует указать в следующем виде:

имя_администратора/код_области, например, *Admin/UG*.

Для возврата в консоль под администратором UGMC необходимо указать имя в следующем виде:

имя_администратора/system, например, Admin/system.`

10.2 Администраторы области

Доступ к веб-консоли управления областью регулируется с помощью создания дополнительных учетных записей администраторов области и назначения им профилей доступа.

Примечание

При создании управляемой области администратор UGMC создает корневого администратора области, обладающего всеми полномочиями на данную зону.

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

Наименование	Описание
Шаг 1. Создать профиль доступа администратора области	В консоли управления областью 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 аутентификации области**. 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 аутентификации области**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль.

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля
Описание	Описание профиля
Права доступа на область	Укажите права доступа на разделы настроек области, такие как администраторы, серверы аутентификации, шаблоны устройств, группы шаблонов, управляемые устройства, журналы и отчеты. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Права доступа на шаблон	Укажите здесь права на просмотр и/или изменение настроек всех или конкретных имеющихся шаблонов. Настройки представлены в виде объектов дерева веб-консоли МЭ UserGate, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись. Например, можно разрешить сетевые настройки одной группе администраторов, а политики МЭ - другой.

10.3 Серверы аутентификации области

Серверы аутентификации - это внешние источники учетных записей пользователей для авторизации в веб-консоли управления области. Работа сервера аутентификации области аналогична работе сервера аутентификации для UGMC, отличие лишь только в месте их использования. Задача серверов аутентификации:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию администраторов областей через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.

SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена или название домена LDAP. Если указано доменное имя, то UserGate получит адрес сервера LDAP с помощью DNS-запроса.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена. Для входа в консоль пользователям LDAP необходимо указывать имя в формате:

domain\user/ realm или *user@domain/ realm*

11 УПРАВЛЕНИЕ МЕЖСЕТЕВЫМИ ЭКРАНАМИ USERGATE

Централизованное управление МЭ UserGate можно разделить на 4 этапа:

1. Создание управляемой области. Смотрите раздел Создание управляемых областей.
2. Создание шаблона или несколько шаблонов, каждый из которых опишет свою часть настроек МЭ. Смотрите раздел Шаблоны устройств для более детальной информации.
3. Объединение необходимых шаблонов в группу шаблонов в требуемом порядке, чтобы получить корректную результирующую настройку УУ. Смотрите раздел Группы шаблонов для более детальной информации.
4. Добавление управляемого устройство (МЭ) и применения к нему группы шаблонов. Смотрите раздел Добавление устройств UserGate под управление UGMC для более детальной информации.

При необходимости настройки, заданные в шаблонах можно изменять, что бы эти отражения применялись ко всем МЭ, к которым применимы данные шаблоны.

UserGate Management Center позволяет создавать и управлять кластеры конфигурации и отказоустойчивости. Подробно тонкости управления кластерами описаны в разделе Кластеризация МЭ UserGate с помощью UserGate Management Center.

11.1 Шаблоны устройств

Шаблон - это базовый блок, с помощью которого можно настроить все параметры работы межсетевого экрана - сетевые настройки, правила межсетевого экрана, контентной фильтрации, системы обнаружения вторжений и других. Для создания шаблона необходимо в разделе **Объекты --> Шаблоны** нажать на кнопку **Добавить** и дать шаблону имя и опциональное описание.

После создания шаблона можно производить настройку его параметров. Для этого необходимо перейти в раздел верхнего меню **Управление шаблонами** и в выпадающем меню выбрать необходимый шаблон.

Настройки параметров шаблона отображаются в виде дерева, полностью аналогично, как они представлены в МЭ UserGate. При настройке параметров следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в МЭ UserGate не будет. В данном случае в МЭ UserGate будет использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор МЭ UserGate.
2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.
3. Правила политик не переопределяют правила, созданные локальным администратором, а добавляются к ним в виде пре- и пост- правил. Подробно о применении правил смотрите раздел данного руководства Шаблоны и группы шаблонов.
4. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования - это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным администратором и необходим для обеспечения первичной связи УУ с UGMC.
5. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо включить чекбокс **Настраивается на устройстве** в настройках сетевого интерфейса.
6. В некоторых настройках и правилах политик доступна опция применения данного правила или настройки только к конкретному устройству. Для этого необходимо выбрать управляемое устройство в свойствах правила/настройки в закладке **Управляемые устройства**. Хотя это и предоставляет

определенную гибкость, следует избегать чрезмерного использования данной опции, поскольку это приводит к сложности понимания применения настроек к группам МЭ UserGate.

7. Библиотеки, например, такие как IP-адреса, списки URL, типы контента и другие, по умолчанию не содержат никакого контента в UGMC в отличие от библиотек, создаваемых по умолчанию на устройствах МЭ UserGate. Для использования библиотек в политиках UGMC, необходимо предварительно добавить элементы в эти библиотеки. Элементы библиотек не участвуют в синхронизации; если список был создан, но не используется в политиках, то данный список не появится в разделе библиотек NGFW.
8. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к УУ. Например, шаблон сетевых настроек, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

11.2 Группы шаблонов

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Результирующие настройки, применяемые к устройству МЭ, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы. Подробнее о результирующих настройках смотрите главу руководства Шаблоны и группы шаблонов.

Для создания группы шаблонов необходимо в разделе **Объекты --> Группы шаблонов** нажать на кнопку **Добавить**, дать группе имя и опциональное описание и добавить в него созданные ранее шаблоны. После добавления шаблонов их можно расположить в требуемом порядке, используя кнопки **Выше**, **Ниже**, **Наверх**, **Вниз**, создав таким образом необходимую результирующую конфигурацию.

11.3 Добавление устройств UserGate под управление UGMC

Группа шаблонов всегда применяется к одному или нескольким управляемым устройствам МЭ UserGate. Процедура добавления УУ в UserGate Management Center состоит из следующих шагов:

Наименование	Описание
Шаг 1. Обеспечить доступ от УУ до UGMC	На сервере UGMC необходимо разрешить сервис **UserGate Management Center** зоне, к которой подключены УУ. Сервер UGMC слушает подключения от УУ на портах TCP 2022 и 9712. Передача данных между сервером UGMC и УУ осуществляется по зашифрованному каналу.
Шаг 2. Создать объект УУ	В консоли управления областью в разделе **Объекты --> Управляемые устройства** нажать кнопку **Добавить** и указать необходимые настройки.
Шаг 3. Связать созданный объект УУ с реальным устройством МЭ UserGate.	В консоли управления МЭ UserGate настройте связь между UGMC и устройством. Данную операцию можно произвести в момент первоначальной установки МЭ UserGate, либо уже на настроенный МЭ. Оба варианта подробно описаны далее в этой главе.

При создании объекта УУ необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект УУ. Если объект УУ включен, то он занимает одну лицензию.
Название	Название для УУ. Можно вводить произвольное название.
Описание	Описание УУ.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому УУ.
Синхронизация	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • **Автоматическая синхронизация** - синхронизация включена. Настройки применяются к устройству. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к УУ, это изменение применяется к МЭ без задержек. • **Отключено** - синхронизация выключена. • **Ручная синхронизация** - режим синхронизации, при котором настройки применяются однократно. Полезно в случаях, когда необходимо изменить много настроек в шаблонах и единовременно отослать их на устройство. В этом случае необходимо отключить синхронизацию, произвести необходимые изменения в шаблонах, после чего включить синхронизацию в режим **Ручная синхронизация**.

Для осуществления связи МЭ с UGMC во время первоначальной настройки МЭ UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Скопировать Код устройства	В UGMC выбрать созданный объект УУ и нажать на кнопку **Показать уникальный код устройства**. Скопировать данный код в буфер обмена.
Шаг 2. На МЭ в момент первоначальной инициализации выбрать установку с помощью UGMC	В момент первоначальной инициализации на этапе задания имени администратора и его пароля необходимо выбрать ссылку **Настроить через UGMC**.
Шаг 3. Указать необходимые настройки нового узла и ввести уникальный код устройства	Указать следующие параметры: • Сетевые настройки данного МЭ UserGate (IP, маска, шлюз). Данные настройки будут применены к указанному интерфейсу. Необходимо, чтобы после задания сетевых настроек появилась сетевая доступность с этого МЭ до сервера UGMC. • Имя локального администратора и его пароль. • IP-адрес сервера UGMC и уникальный код устройства, сохраненный на первом шаге.
Шаг 4. Проверить подключение	После подключения к UGMC МЭ UserGate должен получить все настройки, подготовленные для него в UGMC. В МЭ настройки отображаются со значком

	замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте УУ появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

Для осуществления связи уже настроенного МЭ с UGMC необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Скопировать Код устройства	В UGMC выбрать созданный объект УУ и нажать на кнопку **Показать уникальный код устройства**. Скопировать данный код в буфер обмена.
Шаг 2. Указать IP-адрес сервера UGMC и ввести уникальный код устройства	В разделе **Настройки --> Агент UGMC** выбрать **Настроить**, указать IP-адрес сервера UGMC, вставить уникальный код устройства и включить данное подключение. Для успешного выполнения данного шага необходимо, чтобы была сетевая доступность с этого МЭ до сервера UGMC.
Шаг 3. Проверить подключение	После подключения к UGMC МЭ UserGate должен получить все настройки, подготовленные для него в UGMC. В МЭ настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте УУ появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

После того, как МЭ UserGate успешно добавлен в UGMC администратор УУ может:

Наименование	Описание
Посмотреть расширенную информацию о состоянии УУ	В консоли UGMC необходимо выбрать объект УУ и нажать на кнопку **Показать детальную информацию**. Будет отображена следующая информация о подключенном УУ: • Версия ПО УУ. • ПИН-код УУ. • Серийный номер ПАК. • Время непрерывной работы. • Показатели загрузки устройства - загрузка ЦП, оперативной памяти, своп-файла, количество пользователей, подключенных через УУ.
Подключиться к консоли УУ	В консоли UGMC необходимо выбрать объект УУ и нажать на кнопку **Открыть консоль**. В новом окне откроется консоль МЭ UserGate.
Изменить настройки	В консоли UGMC измените настройки одного из шаблонов, входящего в группу шаблонов, примененного к УУ. Новые настройки будут применены к МЭ UserGate.

11.4 Кластеризация МЭ UserGate с помощью UserGate Management Center

Шаблоны устройств позволяют объединить несколько устройств UserGate в кластер конфигурации с едиными настройками на всех узлах кластера и создать на базе узлов кластера конфигурации один или несколько кластеров отказоустойчивости.

Подробно о различных режимах кластеризации, используемых в UserGate, описано в разделе **Кластеризация и отказоустойчивость** документа **UserGate 6. Руководство администратора**.

11.4.1 Кластер конфигурации

Создание кластера конфигурации, управляемого из UGMC, практически идентично созданию отдельно стоящего кластера. Отличие лишь в том, что первый узел кластера должен быть подключен под управление UGMC до создания кластера конфигурации. Каждому узлу кластера конфигурации, подключаемому в UGMC, назначается **идентификатор узла** - уникальный идентификатор вида *node_1, node_2, node_3* и так далее.

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выполнить первоначальную настройку на первом узле кластера	Смотрите главу **Первоначальная настройка** документа **UserGate 6. Руководство администратора**.
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.
Шаг 5. Подключить первый узел кластера конфигурации в UGMC	Подключение первого узла ничем не отличается от подключения отдельно стоящего устройства UserGate. Процедура подключения подробно описана в разделе Добавление устройств UserGate под управление UGMC. Первому узлу автоматически назначается идентификатор *node_1*.

Шаг 6. Подключить второй узел в кластер	**Важно!** Добавление в кластер конфигурации второго и последующих узлов возможно только при первоначальной инициализации этих узлов. 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 система предложит назначить идентификатор кластера для добавляемого устройства в виде *node_2, node_3, node_4* и так далее. Идентификатор *node_1* уже был закреплен за первым узлом кластера. После назначения идентификатора второй узел будет добавлен в кластер, и все настройки первого узла реплицируются на второй. После успешного добавления узла в кластер, данный узел будет отображаться в качестве второго узла в списке управляемых устройств с выбранным идентификатором.

Настройка добавленного узла, включая настройки интерфейсов, зон, политик фильтрации, может производиться либо локально, либо через политики шаблонов UGMC. Если эти настройки уже были выполнены в шаблонах UGMC на момент подключения второго узла, то они будут применены к добавленному узлу сразу же после его добавления в кластер.

Добавление третьего и последующих узлов в кластер конфигурации выполняется аналогично.

11.4.2 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. Для создания кластера отказоустойчивости с помощью UGMC необходимо выполнение следующих условий:

Наименование	Описание
Наличие кластера конфигурации	Должен быть создан кластер конфигурации. Кластер конфигурации должен корректно отображаться в списке управляемых устройств.
Наличие управляемых из UGMC интерфейсов	Наличие на устройствах UserGate интерфейсов, которые созданы и управляются из UGMC. Виртуальные IP-адреса могут быть назначены только на интерфейсы, которые созданы в шаблонах UGMC.
Выполнение требований, предъявляемых к кластеру отказоустойчивости	Выполнение всех требований, предъявляемых к узлам, при создании кластера отказоустойчивости без использования UGMC. Подробно о кластерах отказоустойчивости описано в разделе **Кластеризация и отказоустойчивость** документа **UserGate 6. Руководство администратора**.

Для создания кластера отказоустойчивости необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере	В одном из шаблонов **UGMC**, где настроены зоны для управляемых устройств, в разделе **Зоны** следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес.
Шаг 2. Создать кластер отказоустойчивости	В одном из шаблонов **UGMC**, в разделе **Управление устройством --> Кластер отказоустойчивости** нажать на кнопку **Добавить** и указать параметры кластера отказоустойчивости.
Шаг 3. 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. Данную настройку можно выполнить в одном из шаблонов **UGMC**, в разделе **Настройки**. Более детально эти параметры описаны в разделе **Настройка устройства** документа **UserGate 6. Руководство администратора**.

Параметры отказоустойчивого кластера:

Наименование	Описание
Вкл	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 UserGate. 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. Узлы кластера представлены идентификаторами, назначенными узлам кластера конфигурации при создании кластера конфигурации.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера. В качестве интерфейсов могут быть использованы только интерфейсы, которые были созданы в одном из шаблонов UGMC.

11.5 Управление обновлениями управляемых устройств

UserGate Management Center позволяет создать централизованную политику обновления программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке (база категорий URL-фильтрации, СОВ, списки IP-адресов, URL, типов контента и другие).

Примечание

После добавления МЭ UserGate под управление UGMC, устройство UserGate автоматически начинает скачивать все обновления с сервера UGMC.

Для управления обновлениями с помощью UGMC необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить расписание проверки обновлений	Расписание проверки устанавливает время и периодичность проверки обновлений. Оно может быть настроено локально на каждом из устройств UserGate, либо централизовано с помощью настройки шаблонов в UGMC. В обоих случаях настройка выполняется идентично. В случае локальной настройки она производится в разделе **Общие настройки** в веб-консоли управления устройством. В случае настройки через UGMC настройка производится в одном из шаблонов в разделе **Общие настройки**. Подробно о настройке расписания обновлений смотрите главу **Общие настройки** документа **UserGate 6. Руководство администратора**.
Шаг 2. Настроить политику обновления ПО для устройств UserGate	Политика обновлений ПО позволяет задать обновление, доступное для установки на все или выборочные УО. Подробно об обновлениях ПО смотрите в разделе Обновление ПО.
Шаг 3. Настроить политику обновления библиотек для устройств UserGate	Политика обновления библиотек позволяет выбрать необходимые обновления библиотек для установки на УО. Подробно об обновлениях библиотек смотрите в разделе Обновление библиотек.

11.5.1 Обновление ПО

Компания UserGate периодически выпускает обновления программного обеспечения МЭ UserGate. Эти обновления выкладываются в репозитарий UserGate (http://static.usergate.com), откуда они уже доступны для скачивания МЭ. Если МЭ UserGate подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений.

В некоторых случаях служба поддержки UserGate может рекомендовать к установке определенным клиентам специфические обновления, недоступные для скачивания из репозитария. Такие обновления следует добавлять в UGMC с помощью импорта обновления из файла.

Порядок установки обновлений, следующий:

Наименование	Описание
Шаг 1. Загрузить обновления в репозитарий UGMC	Загрузить обновления можно либо из репозитария UserGate, либо импортировав файл обновления вручную. Для загрузки обновлений из репозитария необходимо в разделе **Объекты --> Обновления ПО** нажать на кнопку **Выбрать онлайн-обновления**, отобразится список обновлений, доступных для скачивания из репозитария UserGate. Выделить необходимые обновления и нажать кнопку **Выбрать**. Выделенные обновления будут загружены в UGMC. Для загрузки вручную необходимо в разделе **Объекты --> Обновления ПО** нажать на кнопку **Импортировать обновление**, выбрать файл с обновлением. Если для файла обновлений в самом обновлении не указаны название и версия обновления, то необходимо указать их в соответствующих полях. Кнопка **Сохранить** загрузит выбранное обновление в UGMC.
Шаг 2. Утвердить обновление для всех или для конкретных устройств	Для установки обновления на все устройства необходимо выбрать интересующее обновление и нажать на кнопку **Утвердить обновление**. Только одно обновление может быть утверждено для всех устройств. Если требуется установить данное обновление на группу устройств (например, для проведения тестирования), то необходимо в свойствах обновления указать управляемые устройства, для которых данное обновление будет доступно, и установить чекбокс **Утвердить обновление**.
Шаг 3. Провести установку обновления	После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. УО скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли МС или в ручном режиме администратором управляемого устройства.

Обновление в репозитарии UGMC имеет следующие свойства:

Наименование	Описание
Название	Название обновления. Обычно не доступно для изменения, содержится в коде изменения.

Описание	Произвольное описание обновления.
Версия	Версия обновления. Не доступно для изменения, содержится в коде изменения.
Размер	Размер обновления.
Версия релиза	Версия релиза UserGate, для которого это обновление выпущено. Не доступно для изменения, содержится в коде изменения.
Статус	Статус обновления, например, скачано.
Прогресс	Показывает прогресс загрузки обновления с репозитария UserGate.
Канал обновлений	Канал обновлений репозитария UserGate: • Стабильные - канал стабильных обновлений ПО. • Бета - канал экспериментальных обновлений.
Список изменений	Ссылка на список изменений, содержащихся в данном обновлении.
Управляемые устройства	Список управляемых устройств, которым назначено данное обновление.
Добавлено	Дата добавления обновления в репозитарий UGMC и имя администратора, который выполнил добавление.
Утверждено	Дата утверждения обновления и имя администратора, который выполнил утверждение.

11.5.2 Обновление библиотек

Библиотеки - это обновляемые базы ресурсов, предоставляемых по подписке клиентам UserGate (база категорий URL-фильтрации, сигнатуры СОВ, списки IP-адресов, URL, MIME-типов, морфологические базы и другие). Эти обновления выкладываются в репозитарий UserGate (http://static.usergate.com), откуда они уже доступны для скачивания МЭ UserGate. Если МЭ UserGate подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

В случаях, когда UGMC не имеет доступа до репозитария UserGate, имеется возможность импортировать обновление вручную из файла, полученного в личном кабинете клиента UserGate (https://my.usergate.com).

Библиотеки, находящиеся в репозитарии UGMC доступны всем управляемым устройствам UserGate. УО скачивают и устанавливают доступные обновления автоматически в соответствии с расписанием проверки обновлений.

Обновление библиотек в репозитарии UGMC имеет следующие свойства:

Наименование	Описание

Название	Название обновления. Не доступно для изменения, содержится в коде изменения.
Описание	Произвольное описание обновления.
Скачивать	Режим скачивания новых версий. По умолчанию установлен режим **Автоматически** - UGMC автоматически проверяет наличие новых версий в репозитарии UserGate и скачивает их. При выборе режима **Ручное** - UserGate не обновляет выбранную библиотек в автоматическом режиме.
Размер	Размер обновления.
Версия	Версия обновления библиотеки.
Обновлено	Дата и время последнего обновления конкретной библиотеки.

12 ПРИЛОЖЕНИЕ 1. ТРЕБОВАНИЯ К СЕТЕВОМУ ОКРУЖЕНИЮ

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8010	Входящий (до веб-консоли UserGate Management Center)	Доступ к веб-интерфейсу управления устройством.
	TCP	8300	Входящий (до веб-консоли UserGate NGFW, подключённого к UGMC)	Доступ к веб-интерфейсу управления UG NGFW, подключённого к UGMC.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверу технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)	Синхронизация времени.
DNS	UDP	53	Исходящий (от UserGate до DNS-сервера)	Сервис получения информации (IP-адрес) о доменах.
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Доступ до сервера регистрации продуктов UserGate reg2.entensys.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до серверов static.entensys.com.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)

Сервис UserGate Management Center	TCP	9712	Входящий (к UGMC от NGFW)	Первоначальная установка связи и обмен ключами шифрования управляемых устройств и сервера UserGate Management Center.
		2022	Входящий (к UGMC от NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 – для LDAP и 636 - для LDAP over SSL).
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)	Сервис службы DHCP.