

# UserGate 5

## Руководство администратора

# Оглавление

1 Введение .....	7
<b>1.1 Безопасность сети и защита от сетевых угроз .....</b>	<b>7</b>
1.1.1 Межсетевое экранирование.....	7
1.1.2 Обнаружение и предотвращение вторжений.....	7
1.1.3 Защита от DOS-атак и сетевого флуда.....	7
1.1.4 Антивирусная проверка трафика .....	7
1.1.5 Проверка почтового трафика .....	7
1.1.6 Работа с внешними системами безопасности.....	8
1.1.7 Управление АСУ ТП .....	8
1.1.8 Настройка политик безопасности при помощи сценариев .....	8
<b>1.2 Улучшение производительности и надежности интернета .....</b>	<b>8</b>
1.2.1 Поддержка кластеризации и отказоустойчивости .....	8
1.2.2 FTP поверх HTTP.....	8
1.2.3 Поддержка нескольких провайдеров.....	8
1.2.4 Управление пропускной способностью .....	9
1.2.5 Поддержка WCCP.....	9
<b>1.3 Управление трафиком и контроль доступа в интернет.....</b>	<b>9</b>
1.3.1 Маршрутизация трафика и публикация ресурсов.....	9
1.3.2 Авторизация пользователей.....	9
1.3.3 Поддержка гостевого портала.....	9
1.3.4 Проксирование приложений .....	10
1.3.5 Поддержка политики BYOD .....	10
<b>1.4 Контент-фильтрация и контроль приложений .....</b>	<b>10</b>
1.4.1 Интернет-фильтрация.....	10
1.4.2 Выборочная блокировка рекламы .....	10
1.4.3 Активация безопасного поиска .....	10
1.4.4 Блокировка приложений социальных сетей.....	10
1.4.5 Инжектирование кода на веб-страницы.....	11
1.4.6 Инспектирование SSL-трафика .....	11
1.4.7 VPN и веб-портал.....	11
<b>1.5 Журналы и отчеты .....</b>	<b>11</b>
<b>1.6 Другие функции .....</b>	<b>11</b>
1.6.1 Рольевой доступ администраторов к элементам управления UserGate.....	11
1.6.2 Использование оповещений.....	12
1.6.3 Типы интерфейсов .....	12
1.6.4 DNS-фильтрация.....	12
1.6.5 Функция балансировщика нагрузки .....	12
<b>2 Первоначальная настройка .....</b>	<b>13</b>
<b>2.1 Требования к сетевому окружению .....</b>	<b>13</b>
<b>2.2 Развертывание программно-аппаратного комплекса.....</b>	<b>13</b>
<b>2.3 Развертывание виртуального образа.....</b>	<b>13</b>
<b>2.4 Подключение к UserGate .....</b>	<b>14</b>
<b>3 Лицензирование UserGate .....</b>	<b>17</b>
<b>4 Настройка устройства .....</b>	<b>19</b>
<b>4.1 Общие настройки .....</b>	<b>19</b>

<b>4.2 Управление устройством .....</b>	<b>20</b>
4.2.1 Диагностика .....	21
4.2.2 Операции с сервером .....	21
4.2.3 Экспорт настроек .....	22
<b>4.3 Кластеризация и отказоустойчивость .....</b>	<b>24</b>
4.3.1 Кластер конфигурации .....	24
4.3.2 Кластер отказоустойчивости Актив-Пассив .....	26
4.3.3 Кластер отказоустойчивости Актив-Актив .....	28
<b>4.4 Управление доступом к консоли UserGate .....</b>	<b>32</b>
<b>4.5 Управление сертификатами .....</b>	<b>35</b>
4.5.1 Использование корпоративного УЦ для создания сертификата инспектирования SSL .....	39
<b>4.6 Интерфейс командной строки (CLI) .....</b>	<b>40</b>
<b>4.7 Системные утилиты .....</b>	<b>46</b>
<b>5 Настройка сети .....</b>	<b>48</b>
<b>5.1 Настройка зон .....</b>	<b>48</b>
<b>5.2 Настройка интерфейсов .....</b>	<b>50</b>
5.2.1 Создание интерфейса VLAN .....	51
5.2.2 Объединение интерфейсов в бонд .....	52
5.2.3 Создание моста (bridge) .....	54
5.2.4 Интерфейс PPPOE .....	56
5.2.5 Интерфейс VPN .....	57
5.2.6 Интерфейс туннель .....	57
5.2.7 Настройка Netflow .....	58
<b>5.3 Настройка шлюзов .....</b>	<b>59</b>
<b>5.4 Настройка DHCP .....</b>	<b>60</b>
<b>5.5 Настройка DNS .....</b>	<b>61</b>
<b>5.6 Поддержка WCCP .....</b>	<b>62</b>
<b>5.7 Маршруты .....</b>	<b>64</b>
<b>5.8 Протоколы динамической маршрутизации .....</b>	<b>65</b>
5.8.1 OSPF .....	65
5.8.2 BGP .....	68
<b>6 Пользователи и устройства .....</b>	<b>72</b>
<b>6.1 Группы .....</b>	<b>72</b>
<b>6.2 Пользователи .....</b>	<b>73</b>
<b>6.3 Серверы авторизации .....</b>	<b>73</b>
6.3.1 LDAP-коннектор .....	73
6.3.2 Сервер авторизации пользователей Radius .....	75
6.3.3 Сервер авторизации пользователей TACACS+ .....	75
6.3.4 Сервер авторизации пользователей SAML IDP .....	76
6.3.5 Сервер авторизации NTLM .....	78
6.3.6 Метод авторизации Kerberos .....	79
6.3.7 Метод авторизации HTTP Basic .....	81
<b>6.4 Профили авторизации .....</b>	<b>82</b>
<b>6.5 Настройка Captive-портала .....</b>	<b>83</b>
<b>6.6 Профили MFA (мультифакторной аутентификации) .....</b>	<b>87</b>
<b>6.7 Пользователи терминальных серверов .....</b>	<b>90</b>
<b>6.8 Агент авторизации для Windows .....</b>	<b>91</b>
<b>6.9 Прокси-агент для Windows .....</b>	<b>92</b>

<b>6.10 Управление гостевыми пользователями .....</b>	<b>93</b>
<b>6.11 Radius accounting.....</b>	<b>94</b>
<b>6.12 Политики BYOD .....</b>	<b>96</b>
<b>7 Политики сети.....</b>	<b>98</b>
<b>7.1 Межсетевой экран.....</b>	<b>99</b>
<b>7.2 NAT и маршрутизация.....</b>	<b>101</b>
7.2.1 Правила NAT.....	101
7.2.2 Правила DNAT.....	102
7.2.3 Правила порт-форвардинга.....	104
7.2.4 Policy-based routing .....	105
7.2.5 Network mapping .....	107
<b>7.3 Балансировка нагрузки .....</b>	<b>108</b>
<b>7.4 Пропускная способность .....</b>	<b>111</b>
<b>8 Политики безопасности.....</b>	<b>113</b>
<b>8.1 Фильтрация контента .....</b>	<b>113</b>
<b>8.2 Веб-безопасность .....</b>	<b>116</b>
<b>8.3 Инспектирование SSL .....</b>	<b>118</b>
<b>8.4 Система обнаружения и предотвращения вторжений .....</b>	<b>121</b>
<b>8.5 Правила АСУ ТП.....</b>	<b>125</b>
<b>8.6 Сценарии.....</b>	<b>127</b>
<b>8.7 Работа с внешними ICAP-серверами .....</b>	<b>128</b>
<b>8.8 Защита почтового трафика .....</b>	<b>132</b>
<b>8.9 Защита от DoS атак.....</b>	<b>135</b>
<b>9 Глобальный портал .....</b>	<b>138</b>
<b>9.1 Веб-портал (SSL VPN).....</b>	<b>138</b>
<b>9.2 Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси .....</b>	<b>140</b>
<b>10 Настройка VPN.....</b>	<b>144</b>
<b>10.1 VPN для удаленного доступа клиентов (Remote access VPN) .....</b>	<b>144</b>
<b>10.2 VPN для защищенного соединения офисов (Site-to-Site VPN) .....</b>	<b>147</b>
<b>11 Библиотеки элементов .....</b>	<b>152</b>
<b>11.1 Морфология .....</b>	<b>152</b>
<b>11.2 Сервисы.....</b>	<b>155</b>
<b>11.3 IP-адреса .....</b>	<b>155</b>
<b>11.4 Useragent браузеров .....</b>	<b>156</b>
<b>11.5 Типы контента.....</b>	<b>157</b>
<b>11.6 Списки URL.....</b>	<b>158</b>
<b>11.7 Календари.....</b>	<b>161</b>
<b>11.8 Полосы пропускания.....</b>	<b>161</b>
<b>11.9 Профили АСУ ТП .....</b>	<b>161</b>
<b>11.10 Шаблоны страниц .....</b>	<b>162</b>
<b>11.11 Категории URL.....</b>	<b>163</b>
<b>11.12 Измененные категории URL.....</b>	<b>164</b>
<b>11.13 Приложения.....</b>	<b>165</b>

<b>11.14 Почтовые адреса</b> .....	<b>165</b>
<b>11.15 Номера телефонов</b> .....	<b>165</b>
<b>11.16 Профили COB</b> .....	<b>166</b>
<b>11.17 Профили оповещений</b> .....	<b>166</b>
<b>11.18 Профили Netflow</b> .....	<b>167</b>
<b>12 Дашборд</b> .....	<b>169</b>
<b>13 Диагностика и мониторинг</b> .....	<b>170</b>
<b>13.1 Маршруты</b> .....	<b>170</b>
<b>13.2 VPN</b> .....	<b>170</b>
<b>13.3 Веб-портал</b> .....	<b>170</b>
<b>13.4 Захват пакетов</b> .....	<b>171</b>
<b>13.5 Запросы в белый список</b> .....	<b>171</b>
<b>13.6 Трассировка правил</b> .....	<b>172</b>
<b>13.7 Ping</b> .....	<b>173</b>
<b>13.8 Traceroute</b> .....	<b>173</b>
<b>13.9 Запрос DNS</b> .....	<b>174</b>
<b>13.10 Оповещения</b> .....	<b>174</b>
13.10.1 Правила оповещений .....	174
13.10.2 SNMP.....	175
<b>14 Журналы и отчеты</b> .....	<b>177</b>
<b>14.1 Журналы</b> .....	<b>177</b>
14.1.1 Журнал событий.....	177
14.1.2 Журнал веб-доступа .....	177
14.1.3 Журнал трафика.....	178
14.1.4 Журнал COB .....	179
14.1.5 История поиска.....	179
14.1.6 Поиск и фильтрация данных .....	180
14.1.7 Экспорт журналов .....	182
<b>14.2 Отчеты</b> .....	<b>184</b>
14.2.1 Шаблоны отчетов .....	185
14.2.2 Правила отчетов .....	185
14.2.3 Созданные отчеты .....	187
<b>15 Гостевой портал</b> .....	<b>188</b>
<b>16 Помощь</b> .....	<b>189</b>
<b>17 Admin</b> .....	<b>190</b>
<b>18 Приложение 1. Установка сертификата локального удостоверяющего центра</b> .....	<b>191</b>
<b>18.1 Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows</b> .....	<b>191</b>
<b>18.2 Установка сертификата в браузер Safari, Chrome в ОС MacOSX</b> .....	<b>195</b>
<b>18.3 Установка сертификата в браузер Firefox</b> .....	<b>197</b>
<b>19 Приложение №2. Таблица соответствия категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0.</b> .....	<b>200</b>



# 1 ВВЕДЕНИЕ

UserGate представляет собой универсальный интернет-шлюз класса Unified Threat Management (единая защита от угроз), объединяющий в себе межсетевой экран, маршрутизацию, шлюзовую антивирус, систему обнаружения и предотвращения вторжений (COB), VPN-сервер, систему контентной фильтрации, модуль мониторинга и статистики и многие другие функции. Продукт позволяет управлять сетью компании, оптимизировать используемый ею трафик и эффективно предотвращать интернет-угрозы.

## 1.1 Безопасность сети и защита от сетевых угроз

### 1.1.1 Межсетевое экранирование

Встроенный в UserGate межсетевой экран нового поколения (NGFW - Next Generation Firewall) фильтрует трафик, проходящий через определенные протоколы (например, TCP, UDP, IP), тем самым обеспечивая защиту сети от хакерских атак и разнообразных типов вторжений, основанных на использовании данных протоколов.

### 1.1.2 Обнаружение и предотвращение вторжений

Система обнаружения и предотвращения вторжений (COB) позволяет распознавать вредоносную активность внутри сети. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз в режиме реального времени, а также предоставление отчетов.

Администратор может создавать различные COB-профили (наборы сигнатур, релевантных для защиты определенных сервисов) и задавать правила COB, определяющие действия для выбранного типа трафика, который будет проверяться модулем COB в соответствии с назначенными профилями.

### 1.1.3 Защита от DOS-атак и сетевого флуда

UserGate позволяет задать параметры защиты каждой зоны сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP), указав порог уведомления - количество запросов с одного IP-адреса, после которого происходит запись в журнал - и порог отбрасывания пакетов - количество запросов, после которого пакеты отбрасываются с соответствующей записью в журнале.

Возможно настроить исключения, например, для зон, использующих IP-телефонию и поэтому отправляющих большое количество UDP-пакетов.

### 1.1.4 Антивирусная проверка трафика

Потоковый антивирус UserGate позволяет обеспечить антивирусную проверку трафика без ущерба для производительности и быстродействия сети. Модуль использует обширную базу сигнатур.

### 1.1.5 Проверка почтового трафика

UserGate способен обрабатывать транзитный почтовый трафик (SMTP(S), POP3(S)), анализируя его источник, а также содержание письма и вложений, что гарантирует надежную защиту от спама, вирусов,

pharming- и phishing- атак. UserGate также предоставляет возможность гибкой настройки фильтрации почтового трафика по группам пользователей.

### **1.1.6 Работа с внешними системами безопасности**

Имеется возможность передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. Администратор может указать, какой трафик требуется передавать на ICAP, а также настроить работу с фермами серверов.

### **1.1.7 Управление АСУ ТП**

В новой версии платформы появилась возможность настройки автоматизированной системы управления технологическим производством (АСУ ТП) и управления ей. Администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий. Это позволяет автоматизировать основные операции технологического процесса, сохраняя при этом возможность контроля и вмешательства человека при необходимости.

### **1.1.8 Настройка политик безопасности при помощи сценариев**

UserGate позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря автоматизации безопасности при помощи механизма сценариев (SOAR - Security Orchestration, Automation and Response).

Эта концепция находится на пике популярности и позволяет администратору создавать сценарии (запускаемые по плану или при обнаружении атаки), где прописываются автоматические действия в ответ на те или иные события. Такой подход обеспечивает гибкую настройку политик безопасности, сокращает участие человека благодаря автоматизации повторяющихся задач, а также дает возможность приоритезировать сценарии для скорейшей реакции на критичные угрозы.

## **1.2 Улучшение производительности и надежности интернета**

### **1.2.1 Поддержка кластеризации и отказоустойчивости**

UserGate поддерживает 2 типа кластеров: кластер конфигурации, позволяющий задать единые настройки узлам в рамках кластера, и кластер отказоустойчивости, призванный обеспечить бесперебойную работу сети. Кластер отказоустойчивости может работать в двух режимах: Актив-Актив и Актив-Пассив. Оба режима поддерживают синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другие.

### **1.2.2 FTP поверх HTTP**

Модуль FTP поверх HTTP позволяет обращаться к содержимому FTP-сервера из браузера пользователя.

### **1.2.3 Поддержка нескольких провайдеров**

При подключении системы к нескольким провайдерам UserGate позволяет настроить для каждого из них свой шлюз для обеспечения доступа к интернету. Администратор также может настроить балансировку

трафика между провайдерами, указав вес каждого шлюза, или указать один из шлюзов как основной с переключением на других провайдеров в случае недоступности основного шлюза.

### 1.2.4 Управление пропускной способностью

Правила управления пропускной способностью служат для ограничения канала для определенных пользователей, хостов, сервисов или приложений.

### 1.2.5 Поддержка WCCP

Поддержка протокола WCCP позволяет использовать UserGate в инфраструктуре с WCCP-северами, например, маршрутизаторами Cisco.

## 1.3 Управление трафиком и контроль доступа в интернет

### 1.3.1 Маршрутизация трафика и публикация ресурсов

UserGate позволяет использовать как статическую, так и динамическую маршрутизацию. Динамическая маршрутизация осуществляется по протоколам OSPF и BGP, что позволяет использовать UserGate в сложной маршрутизируемой сети предприятия.

Администратор может создавать в системе правила NAT (для предоставления пользователям доступа в интернет), а также правила безопасной публикации внутренних ресурсов в интернет с использованием reverse-прокси для HTTP/HTTPS и DNAT для других протоколов.

### 1.3.2 Авторизация пользователей

Платформа поддерживает различные механизмы авторизации пользователей: Captive-портал, Kerberos, NTLM, при этом учетные записи могут поступать из различных источников - LDAP, Active directory, FreeIPA, TACACS+, Radius, SAML IDP. Авторизация SAML IDP, Kerberos или NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory.

Администратор может настроить правила безопасности, ширину канала, правила межсетевого экранирования, контентной фильтрации и контроля приложений для отдельных пользователей, групп пользователей, а также всех известных или неизвестных пользователей. Дополнительно к этому продукт поддерживает применение правил безопасности к пользователям терминальных служб с помощью специальных агентов (Terminal Services Agents), а также использование агента авторизации для Windows-платформ.

Для обеспечения большей безопасности учетных записей рекомендуется использовать мультифакторную аутентификацию с помощью токенов TOTP (Time-based One Time Password Algorithm), SMS или электронной почты.

### 1.3.3 Поддержка гостевого портала

UserGate позволяет предоставлять пользователям временный доступ к сети, что актуально, например, для публичных Wi-Fi сетей. Профили могут быть как созданы администратором, так и зарегистрированы самими пользователями с подтверждением через e-mail или SMS. Платформа позволяет указывать отдельные настройки безопасности для временных пользователей.

### 1.3.4 Проксирование приложений

Для пользователей, работающих с ОС Windows, можно настроить прокси-агент, позволяющий использовать возможности прокси приложениям, не умеющим работать с прокси-серверами. Прокси-агент также может быть использован для предоставления таким приложениям доступа в интернет в случаях, когда UserGate не является шлюзом по умолчанию.

### 1.3.5 Поддержка политики BYOD

Концепция BYOD (Bring Your Own Device) продолжает набирать популярность, ставя перед системами безопасности новые задачи. UserGate позволяет настроить гибкие политики доступа в сеть для различных групп пользователей и типов устройств, а также ограничить количество устройств, используемых одним пользователем.

## 1.4 Контент-фильтрация и контроль приложений

### 1.4.1 Интернет-фильтрация

Использование модуля интернет-фильтрации обеспечивает административный контроль за использованием интернета, загружаемыми данными. Модуль обеспечивает блокировку посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой.

Для анализа безопасности сайтов, запрашиваемых пользователями, используются репутационные сервисы, типы контента (фото, видео, тексты и др.), специальные морфологические словари, предоставляемые UserGate, а также черные и белые списки URL и Useragent, с помощью которых администратор может запретить или разрешить работу с определенным типом браузеров. UserGate предоставляет возможность создавать собственные черные и белые списки, словари, типы контента, морфологические словари и Useragent, применяя их как правила к пользователям и группам пользователей.

### 1.4.2 Выборочная блокировка рекламы

Даже безопасные сайты могут содержать нежелательные изображения на баннерах, содержимое которых не зависит от владельца ресурса. UserGate решает эту проблему, блокируя баннеры и защищая пользователей от негативного контента.

### 1.4.3 Активация безопасного поиска

UserGate позволяет принудительно активировать функцию безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. Такая защита позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту. Также можно заблокировать поисковые системы, в которых не реализована функция безопасного поиска.

### 1.4.4 Блокировка приложений социальных сетей

UserGate дает возможность блокировки игр и других приложений для наиболее популярных социальных сетей, таких, как Facebook, VK, Одноклассники. Администраторы могут разрешать использование социальных сетей в целом, при этом контролируя и ограничивая непродуктивные действия.

## 1.4.5 Инжектирование кода на веб-страницы

Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователями. Эта возможность может быть использована для получения различных метрик, сокрытия некоторых элементов веб-страниц, а также показа рекламы или другой информации.

## 1.4.6 Инспектирование SSL-трафика

Платформа UserGate позволяет фильтровать не только обычный, но и зашифрованный трафик (протоколы HTTPS, SMTPS, POP3S), дешифруя их при помощи технологии MITM (Man In The Middle) и подписывая доверенным корневым сертификатом с последующим шифрованием после анализа. Система позволяет настроить выборочную проверку трафика, например, не расшифровывать ресурсы категории «Финансы».

## 1.4.7 VPN и веб-портал

VPN (Virtual Private Network) служит для того, чтобы настраивать виртуальные логические сети поверх других сетей, например, интернет. UserGate поддерживает два типа VPN-сетей: Remote Access VPN (модель клиент-сервер) и Site-to-Site VPN (модель сервер-сервер).

Для создания туннелей используется протокол Layer 2 Tunneling Protocol (L2TP), а для защиты передаваемых данных - протокол IPSec. UserGate поддерживает работу со стандартными клиентами большинства популярных операционных систем: Windows, Linux, Mac OS X, iOS, Android и других.

Веб-портал (SSL VPN) позволяет предоставить безопасный доступ сотрудникам компании к внутренним веб-ресурсам, серверам SSH и серверам терминальных служб без необходимости установки специального клиента VPN, используя только протокол HTTPS.

## 1.5 Журналы и отчеты

Платформа позволяет осуществлять мониторинг работы системы в режиме реального времени при помощи журналов событий, веб-доступа, COB и трафика. Для удобства анализа администратор может настроить автоматический экспорт журналов на сервера SSH, FTP и Syslog. С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

## 1.6 Другие функции

### 1.6.1 Ролевой доступ администраторов к элементам управления UserGate

По умолчанию в системе существует один суперадминистратор, который может создавать учетные записи других администраторов и выдавать им права на просмотр и изменение различных разделов.

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

## 1.6.2 Использование оповещений

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается как управление с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps).

Помимо этого, система позволяет создавать профили оповещений, уведомляющие пользователей об определенных событиях по протоколам SMTP (e-mail) и SMPP (SMS).

## 1.6.3 Типы интерфейсов

UserGate позволяет добавлять и настраивать тегированные VLAN-интерфейсы, а также объединять ряд физических интерфейсов в один логический агрегированный интерфейс (бонд) с использованием протокола LACP (link aggregation control protocol) для повышения пропускной способности или для отказоустойчивости канала. Помимо этого, существует возможность объединения интерфейсов в мост (bridge) для осуществления фильтрации трафика на уровне L2 без внесения изменений в сетевую инфраструктуру компании.

## 1.6.4 DNS-фильтрация

UserGate позволяет осуществлять настройку работы с DNS-серверами, а также настраивать сервис DNS-прокси, позволяющий перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора. Платформа также позволяет подключить фильтрацию DNS-запросов пользователей.

## 1.6.5 Функция балансировщика нагрузки

UserGate позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена для внутренних серверов, публикуемых в интернет (DNAT или reverse-прокси), внутренних серверов без публикации, а также для балансировки трафика, пересылаемого на внешние серверы или ферму ICAP-серверов.

## 2 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

UserGate 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 поставляется с четырьмя Ethernet-интерфейсами. В случае поставки в виде ПАК UserGate может содержать от 2 до 64 Ethernet-портов.

### 2.1 Требования к сетевому окружению

Для корректной работы МЭ UserGate должен иметь доступ до следующих серверов, расположенных в сети интернет:

- Сервер регистрации - reg2.entensys.com, порты TCP 80, 443.
- Сервер обновления списков и ПО UserGate - static.entensys.com, порты TCP 80, 443.

При создании кластера конфигурации необходимо обеспечить прохождение следующих протоколов между узлами:

- Обеспечение репликации настроек - порты TCP 4369, TCP 9000-9100.
- Сервис веб-консоли - TCP 8001.

### 2.2 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](#) для дальнейшей настройки.

### 2.3 Развертывание виртуального образа

UserGate 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
<b>Шаг 1.</b> Скачайте образ и распакуйте	Скачайте последнюю версию виртуального образа с официального сайта <a href="https://www.usergate.com/ru">https://www.usergate.com/ru</a> .

<p><b>Шаг 2.</b> Импортируйте образ в свою систему виртуализации</p>	<p>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, <b>после чего отключить службы интеграции</b> в настройках созданной виртуальной машины.</p>
<p><b>Шаг 3.</b> Настройте параметры виртуальной машины</p>	<p>Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb и добавьте по 1Gb на каждые 100 пользователей.</p>
<p><b>Шаг 4.</b> Важно! Увеличьте размер диска виртуальной машины</p>	<p>Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 200Gb или более. Рекомендованный размер - 300Gb или более.</p>
<p><b>Шаг 5.</b> Настройте виртуальные сети</p>	<p>UserGate поставляется с четырьмя интерфейсами, назначенными в зоны:</p> <ul style="list-style-type: none"> <li>• Management - первый интерфейс виртуальной машины</li> <li>• Trusted - второй интерфейс виртуальной машины</li> <li>• Untrusted - третий интерфейс виртуальной машины</li> <li>• DMZ - четвертый интерфейс виртуальной машины.</li> </ul>
<p><b>Шаг 6.</b> Выполните сброс к заводским настройкам</p>	<p>Запустите виртуальную машину UserGate .</p> <p>Во время загрузки выберите <b>Support Menu</b> и выполните <b>Factory reset</b>. <b>Этот шаг крайне важен</b>. Во время этого шага USERGATE настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте.</p>

## 2.4 Подключение к UserGate

Интерфейс eth0 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 eth0.

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
<p><b>Шаг 1.</b> Подключиться к интерфейсу управления</p>	<p><b>При наличии DHCP-сервера</b></p> <p>Подключить интерфейс eth0 в сеть предприятия с работающим DHCP-сервером. Включить UserGate. После загрузки UserGate укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта.</p> <p><b>Статический IP-адрес</b></p> <p>Включить UserGate. Используя CLI (Command Line Interface), назначить необходимый</p>

	<p>IP-адрес на интерфейс eth0. Детали использования CLI смотрите в главе <a href="#">Интерфейс командной строки (CLI)</a>. Подключиться к веб-консоли UserGate по указанному адресу, он должен выглядеть примерно следующим образом:  <a href="https://UserGate_IP_address:8001">https://UserGate_IP_address:8001</a></p>
<b>Шаг 2.</b> Выбрать язык	Выбрать язык, на котором будет продолжена первоначальная настройка.
<b>Шаг 3.</b> Задать пароль	Задать логин и пароль для входа в веб-интерфейс управления.
<b>Шаг 4.</b> Зарегистрировать систему	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ UserGate в интернет. Если на данном этапе выполнить регистрацию не удастся, то ее следует повторить после настройки сетевых интерфейсов на шаге 10.
<b>Шаг 5.</b> Настроить зоны, IP-адреса интерфейсов, подключить UserGate в сеть предприятия	<p>В разделе <b>Интерфейсы</b> включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе <a href="#">Настройка интерфейсов</a>. Система поставляется с предопределенными зонами:</p> <ul style="list-style-type: none"> <li>• Зона Management (сеть управления), интерфейс eth0</li> <li>• Зона Trusted (LAN)</li> <li>• Зона Untrusted (Internet)</li> <li>• Зона DMZ</li> <li>• Зона Cluster</li> <li>• Зона VPN for remote access</li> <li>• Зона VPN for Site-to-Site.</li> </ul>
<b>Шаг 6.</b> Настроить шлюз в интернет	<p>В разделе <b>Шлюзы</b> указать IP-адрес шлюза в интернет на интерфейсе, подключенном в интернет, зона <b>Untrusted</b>.</p> <p>Подробно об управлении шлюзами читайте в главе <a href="#">Настройка шлюзов</a>.</p>
<b>Шаг 7.</b> Указать системные DNS-серверы	<p>В разделе <b>DNS</b> укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации.</p> <p>Подробно об управлении DNS читайте в главе <a href="#">Настройка DNS</a>.</p>
<b>Шаг 8.</b> Создать правила NAT	<p>В разделе <b>NAT и Маршрутизация</b> создать необходимые правила NAT. Для доступа в интернет пользователей сети <b>Trusted</b> правило NAT уже создано - «<b>Trusted --&gt; Untrusted</b>».</p> <p>Подробно о правилах NAT читайте в главе <a href="#">Правила NAT</a>.</p>
<b>Шаг 9.</b> Создать правила межсетевого экрана	<p>В разделе <b>Межсетевой экран</b> создать необходимые правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети <b>Trusted</b> правило межсетевого экрана уже создано - «<b>Internet for Trusted</b>», необходимо только включить его.</p> <p>Подробно о правилах межсетевого экрана читайте в главе <a href="#">Межсетевой экран</a>.</p>
<b>Шаг 10.</b> 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.

	<p>Более подробно о лицензировании продукта читайте в главе <a href="#">Лицензирование UserGate</a>.</p>
<p><b>Шаг 11.</b> Создать дополнительных администраторов (опционально)</p>	<p>В разделе <b>Администраторы UserGate</b> создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).</p>
<p><b>Шаг 12.</b> Настроить авторизацию пользователей (опционально)</p>	<p>В разделе <b>Пользователи и устройства</b> создать необходимые методы авторизации пользователей. Самый простой вариант - это создать локальных пользователей UserGate с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя <b>Any</b> во всех правилах).</p> <p>Для других вариантов авторизации пользователей смотрите главу <a href="#">Пользователи и устройства</a>.</p>
<p><b>Шаг 13.</b> Создать правила контентной фильтрации (опционально)</p>	<p>В разделе <b>Фильтрация контента</b> создать правила фильтрации HTTP(S).</p> <p>Более подробно о фильтрации контента читайте в главе <a href="#">Фильтрация контента</a>.</p>
<p><b>Шаг 14.</b> Создать правила веб-безопасности (опционально)</p>	<p>В разделе <b>Веб-безопасность</b> создать дополнительные правила защиты веб.</p> <p>Более подробно о веб-безопасности читайте в главе <a href="#">Веб-безопасность</a>.</p>
<p><b>Шаг 15.</b> Создать правила инспектирования SSL (опционально)</p>	<p>В разделе инспектирование SSL создать правила для перехвата и расшифровывания HTTPS-трафика. Более подробно о дешифровании HTTPS читайте в главе <a href="#">Инспектирование SSL</a>.</p>

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

## 3 ЛИЦЕНЗИРОВАНИЕ USERGATE

UserGate лицензируется по количеству одновременно подключенных устройств, включая пользователей терминальных серверов, за исключением устройств, чей трафик проходит через UserGate с использованием правил публикации DNAT, Reverse-прокси, веб-портала, защиты почтового трафика.

Например, 100-пользовательская лицензия разрешает подключение к сети одновременно 100 устройствам с уникальными IP-адресами. 101 и следующие устройства не смогут получить доступ к сети. Количество учетных записей пользователей в системе не ограничивается. Лицензия на UserGate дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

Наименование	Описание
<b>Модуль Security Update (SU)</b>	<p>Модуль SU дает право на получение:</p> <ul style="list-style-type: none"><li>• обновлений ПО UserGate</li><li>• обновлений сигнатур системы обнаружения вторжений</li><li>• обновлений сигнатур приложений L7</li><li>• технической поддержки</li></ul> <p>Модуль выписывается на 1 год, по истечении данного срока для получения обновлений ПО и технической поддержки необходимо приобрести продление лицензии.</p>
<b>Модуль Advanced Threat Protection (ATP)</b>	<p>Модуль ATP включает в себя следующие опции:</p> <ul style="list-style-type: none"><li>• годовая подписка на базу категорий сайтов UserGate URL filtering</li><li>• годовая подписка на обновляемые списки запрещенных сайтов Роскомнадзора, список phishing-сайтов, Белый список UserGate, Черный список UserGate</li><li>• годовая подписка на морфологические базы, предоставляемые компанией UserGate</li><li>• годовая подписка на потоковый антивирус UserGate</li><li>• годовая подписка на модуль блокировки рекламы.</li></ul> <p>Модуль выписывается на 1 год, по истечении данного срока:</p> <ul style="list-style-type: none"><li>• UserGate URL filtering перестает работать</li><li>• фильтрация с помощью морфологии перестает работать</li><li>• списки запрещенных сайтов Роскомнадзора, список phishing-сайтов, Белый список UserGate, Черный список UserGate продолжает работать, но обновления недоступны</li><li>• антивирус UserGate перестает работать</li><li>• модуль блокировки рекламы перестает работать</li></ul>
<b>Модуль Mail security</b>	<p>Mail security включает в себя годовую подписку на проверку почтового трафика с помощью модуля антиспама UserGate.</p>

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Перейти в Дашборд	Нажать на пиктограмму <b>Дашборд</b> в правом верхнем углу.
<b>Шаг 2.</b> В разделе <b>Информация о лицензии</b> зарегистрировать продукт	В разделе <b>Информация о лицензии</b> нажать на ссылку <b>Зарегистрированная версия</b> , ввести ПИН-код и заполнить регистрационную форму.

## 4 НАСТРОЙКА УСТРОЙСТВА

### 4.1 Общие настройки

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

Наименование	Описание
<b>Часовой пояс</b>	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.
<b>Язык интерфейса по умолчанию</b>	Язык, который будет использоваться по умолчанию в консоли
<b>Режим авторизации веб-консоли</b>	Способ аутентификации пользователя (администратора) при входе в веб-консоль управления. Возможны следующие варианты: <ul style="list-style-type: none"><li>• <b>По имени и паролю.</b> Администратор должен ввести имя и пароль для получения доступа к веб-консоли</li><li>• <b>По X.509-сертификату.</b> Для авторизации по сертификату необходимо иметь сертификат пользователя, подписанный сертификатом удостоверяющего центра веб-консоли и установленный в браузер. При включении этого режима авторизации режим авторизации по имени и паролю отключается. Вернуть режим авторизации по имени и паролю можно с помощью команд CLI</li></ul>
<b>Модули</b>	Позволяет настроить модули UserGate: <ul style="list-style-type: none"><li>• <b>HTTP(S)-прокси порт</b> - позволяет указать нестандартный номер порта, который будет использоваться для подключения к встроенному прокси-серверу. По умолчанию используется порт TCP 8090.</li><li>• Важно! Нельзя использовать следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.</li><li>• <b>Домен auth captive-портала</b> - служебный домен, который используется UserGate при авторизации пользователей через Captive-портал. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя auth.captive, которое может быть изменено на другое доменное имя, принятое в организации</li><li>• <b>Домен logout captive-портала</b> - служебный домен, который используется пользователями UserGate для окончания сессии (logout). Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя logout.captive, которое может быть изменено на другое доменное имя, принятое в организации</li><li>• <b>Домен страницы блокировки</b> - служебный домен, который используется для отображения страницы блокировки пользователям. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса</li></ul>

	<p>UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то резолвинг настроен автоматически. По умолчанию используется имя block.captive, которое может быть изменено на другое доменное имя, принятое в организации</p> <ul style="list-style-type: none"> <li>• <b>FTP поверх HTTP</b> - включение или отключение модуля, позволяющего получать доступ к содержимым FTP-серверов из пользовательского браузера.</li> <li>• Требуется явное указание прокси-сервера для протокола FTP в браузере пользователя.</li> <li>• Администратор может ограничивать доступ к ресурсам FTP с помощью правил контентной фильтрации (только по условиям Пользователи и URL)</li> <li>• <b>FTP поверх HTTP домен</b> - служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то резолвинг настроен автоматически. По умолчанию используется имя ftpclient.captive, которое может быть изменено на другое доменное имя, принятое в организации</li> </ul>
<p><b>Настройка кэширования HTTP</b></p>	<p>Настройка кэша прокси-сервера:</p> <ul style="list-style-type: none"> <li>• <b>Включен/Выключен</b> - включение или отключение кэширования</li> <li>• <b>Исключения кэширования</b> - список URL, которые не будут кэшироваться</li> <li>• <b>Максимальный размер объекта</b>, Мбайт - объекты с размером более, чем указано в данной настройке, не будут кэшироваться. Рекомендуется оставить значение по умолчанию - 1 Мбайт</li> <li>• <b>Размер RAM-кэша</b>, Мбайт - размер оперативной памяти, отведенный под кэширование. Не рекомендуется ставить более 20% от объема оперативной памяти системы</li> </ul>
<p><b>Log Analyzer</b></p>	<p>Настройки модуля Log Analyzer:</p> <ul style="list-style-type: none"> <li>• <b>Состояние</b> - показывает текущее состояние сервиса статистики.</li> <li>• <b>Локальный сервер/Внешний сервер</b>. Выберите внешний сервер, если у вас есть внешний сервер Log Analyzer, в противном случае выберите локальный сервер.</li> <li>• <b>Порт</b> - порт TCP, на котором слушает внешний сервер Log Analyzer.</li> <li>• <b>Пароль</b> - строка авторизации для подключения к внешнему сервису Log Analyzer.</li> <li>• <b>Журналы --&gt; Журнал событий</b> - отправлять события журнала событий на сервер Log Analyzer.</li> <li>• <b>Журналы --&gt; Журнал COB</b> - отправлять события журнала COB на сервер Log Analyzer.</li> <li>• <b>Журналы --&gt; Журнал трафика</b> - отправлять события журнала трафика на сервер Log Analyzer.</li> <li>• <b>Журналы --&gt; Журнал веб-доступа</b> - отправлять события журнала веб-доступа на сервер Log Analyzer.</li> </ul>

## 4.2 Управление устройством

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

- Кластеризация
- Настройки диагностики

- Операции с сервером
- Экспорт настроек

Возможности кластеризации устройств UserGate описаны в разделе [Кластеризация и отказоустойчивость](#).

### 4.2.1 Диагностика

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

Наименование	Описание
<b>Детализация диагностики</b>	<ul style="list-style-type: none"> <li>• <b>Off</b> - ведение журналов диагностики отключено</li> <li>• <b>Error</b> - журналировать только ошибки работы сервера</li> <li>• <b>Warning</b> - журналировать только ошибки и предупреждения</li> <li>• <b>Info</b> - журналировать только ошибки, предупреждения и дополнительную информацию</li> <li>• <b>Debug</b> - максимум детализации</li> </ul> <p>Рекомендуется установить значение параметра <b>Детализация диагностики</b> в <b>Error</b> (только ошибки) или <b>Off</b> (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность UserGate</p>
<b>Журналы диагностики</b>	<ul style="list-style-type: none"> <li>• <b>Скачать журналы</b> - скачать диагностические журналы для передачи их в службу поддержки UserGate.</li> <li>• <b>Очистить журналы</b> - очистить содержимое журналов.</li> </ul>
<b>Удаленный помощник</b>	<ul style="list-style-type: none"> <li>• <b>Вкл/Выкл</b> - включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UserGate для диагностики и решения проблем. Для успешной активации удаленного помощника UserGate должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH.</li> <li>• <b>Идентификатор удаленного помощника</b> - полученное случайным образом значение. Уникально для каждого включения удаленного помощника</li> <li>• <b>Токен удаленного помощника</b> - полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника</li> </ul>

### 4.2.2 Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
<b>Операции с сервером</b>	<ul style="list-style-type: none"> <li>• <b>Перезагрузить</b> - перезагрузка сервера UserGate</li> <li>• <b>Выключить</b> - выключение сервера UserGate</li> </ul>

Обновления	Выбор канала обновлений ПО UserGate <ul style="list-style-type: none"> <li>• <b>Стабильные</b> - проверка наличия стабильных обновлений ПО</li> <li>• <b>Бета</b> - проверка наличия экспериментальных обновлений.</li> </ul>
------------	---

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

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать файл резервного копирования	Создать резервную копию состояния UserGate, как это описано в разделе <a href="#">Системные утилиты</a> . 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.
<b>Шаг 2.</b> Установить обновления	В разделе <b>Управление устройством</b> при наличии оповещения <b>Доступны новые обновления</b> нажать на ссылку <b>Установить сейчас</b> . Система установит скачанные обновления, по окончании установки UserGate будет перезагружен.



### Примечание

Для обновления узлов кластера конфигурации необходимо, чтобы все узлы были включены и доступны на момент обновления первого узла. Узлы, недоступные на момент обновления первого узла, после обновления необходимо будет добавить в кластер заново.

## 4.2.3 Экспорт настроек

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

## **Примечание**

Экспорт/импорт настроек не восстанавливает состояние кластера, настройки интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать UserGate с помощью имеющегося ПИН-кода, настроить интерфейсы и заново создать кластер, если это необходимо.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Экспорт настроек	В разделе <b>Управление устройством</b> нажать на ссылку <b>Экспорт настроек --&gt; Экспорт</b> . Система сохранит текущие настройки сервера под именем database.bin

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Импорт настроек	В разделе <b>Управление устройством</b> нажать на ссылку <b>Экспорт настроек --&gt; Импорт</b> 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.

## **Примечание**

Время в экспорте настроек по расписанию указывается в часовом поясе UTC.

Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать правило экспорта	В разделе <b>Управление устройством --&gt; Экспорт настроек</b> нажать кнопку <b>Добавить</b> , указать имя и описание правила
<b>Шаг 2.</b> Указать параметры удаленного сервера	Во вкладке правила <b>Удаленный сервер</b> указать параметры удаленного сервера: <ul style="list-style-type: none"><li>• <b>Тип сервера</b> - FTP или SSH</li><li>• <b>Адрес сервера</b> - IP-адрес сервера</li><li>• <b>Порт</b> - порт сервера</li><li>• <b>Логин</b> - учетная запись на удаленном сервере</li><li>• <b>Пароль/Подтверждение пароля</b> - пароль учетной записи</li><li>• <b>Путь на сервере</b> - путь на сервере, куда будут выгружены настройки</li></ul>

<p><b>Шаг 3.</b> Выбрать расписание выгрузки</p>	<p>Во вкладке правила <b>Расписание</b> указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде:</p> <p>(минуты:0-59) (часы:0-23) (дни месяца:0-31) (месяц:0-12) (день недели:0-6, 0-воскресенье)</p> <p>Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"> <li>• Звездочка (*)- обозначает весь диапазон (от первого до последнего);</li> <li>• Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7;</li> <li>• Списки. Это числа (или диапазоны) разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23";</li> <li>• 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."</li> </ul>
--	--

## 4.3 Кластеризация и отказоустойчивость

UserGate поддерживает 2 типа кластеров:

1. **Кластер конфигурации.** Узлы, объединенные в кластер конфигурации, поддерживают единые настройки в рамках кластера.
2. **Кластер отказоустойчивости.** До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив. Возможно собрать несколько кластеров отказоустойчивости.

### 4.3.1 Кластер конфигурации

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

Наименование	Описание
<p>Настройки, уникальные для каждого узла</p>	<p>Настройки Log Analyzer</p> <p>Настройки диагностики</p> <p>Настройки интерфейсов</p> <p>Настройки шлюзов</p> <p>Настройки DHCP</p> <p>Маршруты</p> <p>Настройки OSPF</p> <p>Настройки BGP</p>

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Выполнить первоначальную настройку на первом узле кластера	Смотрите главу <a href="#">Первоначальная настройка</a> .
<b>Шаг 2.</b> Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера	<p>В разделе <b>Зоны</b> создать выделенную зону для репликации настроек кластера или использовать существующую (<b>Cluster</b>). В настройках зоны разрешить следующие сервисы:</p> <ul style="list-style-type: none"> <li>• Консоль администрирования</li> <li>• Кластер</li> </ul> <p>Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.</p>
<b>Шаг 3.</b> Указать IP-адрес, который будет использоваться для связи с другими узлами кластера	В разделе <b>Управление устройством</b> в окне <b>Кластер конфигурации</b> выбрать текущий узел кластера и нажать на кнопку <b>Редактировать</b> . Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
<b>Шаг 4.</b> Сгенерировать <b>Секретный код</b> на первом узле кластера	В разделе <b>Управление устройством</b> нажать на кнопку <b>Сгенерировать секретный код</b> . Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.
<b>Шаг 5.</b> Подключить второй узел в кластер	<p>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.</p> <p>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.</p> <p>Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку <b>Подключить</b>. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и все настройки первого кластера реплицируются на второй.</p>
<b>Шаг 6.</b> Назначить зоны интерфейсам второго узла	В веб-консоли второго узла кластера в разделе <b>Сеть --&gt; Интерфейсы</b> необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера.
<b>Шаг 7.</b> Настроить параметры, индивидуальные для каждого узла кластера (опционально)	Настроить шлюзы, маршруты, параметры OSPF, BGP, индивидуальные для каждого из узлов.

До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько, например, в кластер конфигурации добавлены узлы А, В, С и D на основе которых создано 2 кластера отказоустойчивости - А-В и С-D.

Поддерживаются 2 режима кластера отказоустойчивости - **Актив-Актив** и **Актив-Пассив**.

### 4.3.2 Кластер отказоустойчивости Актив-Пассив

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

#### Примечание

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

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

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

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

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

#### Примечание

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

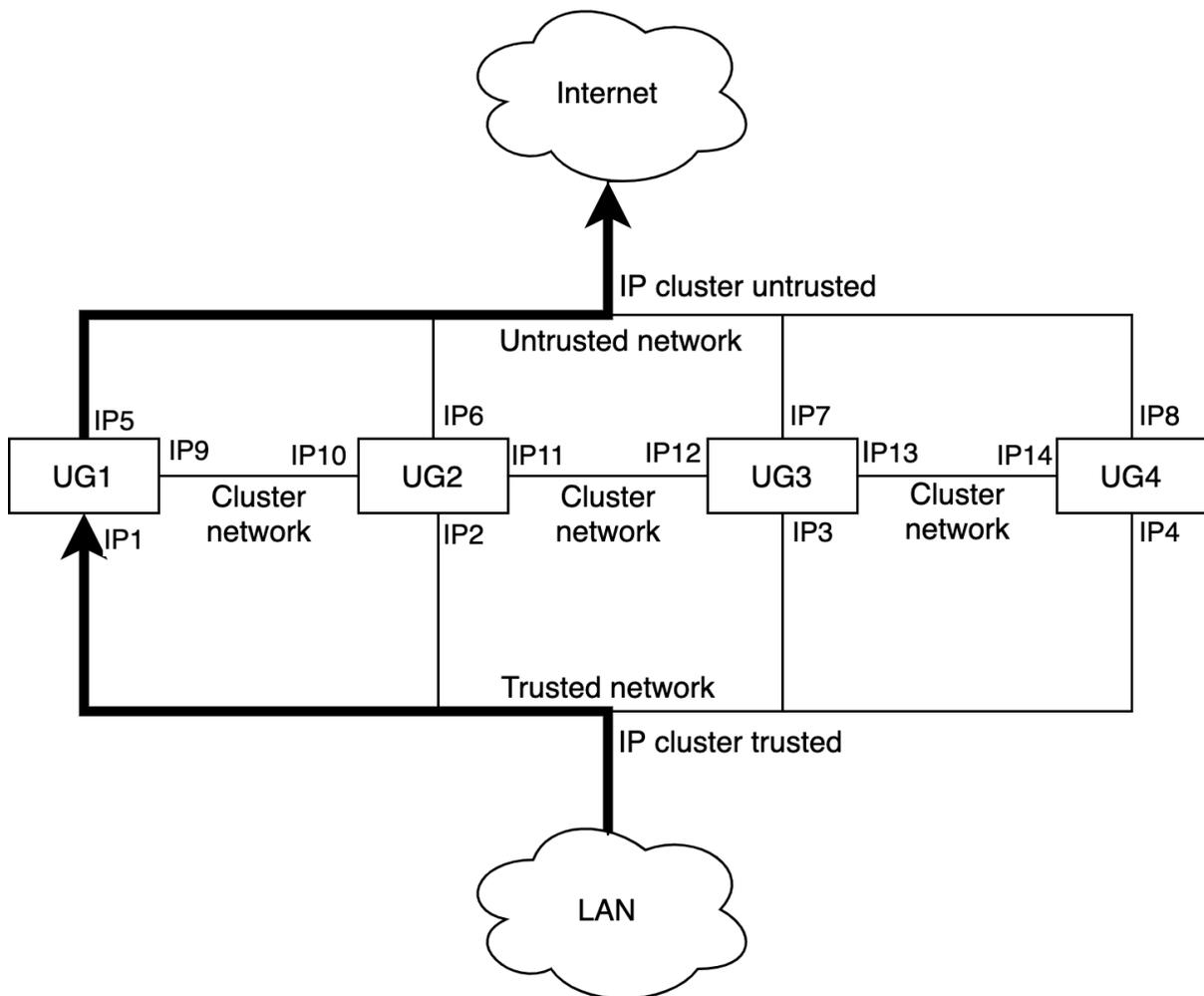
**Примечание**

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

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

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

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



*Отказоустойчивый кластер в режиме Актив-Пассив*

### 4.3.3 Кластер отказоустойчивости Актив-Актив

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

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



#### Примечание

Режим Актив-Актив в отличие от режима Актив-Пассив не поддерживает синхронизацию пользовательских сессий.

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

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

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

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

---

**i** **Примечание**

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

---

**i** **Примечание**

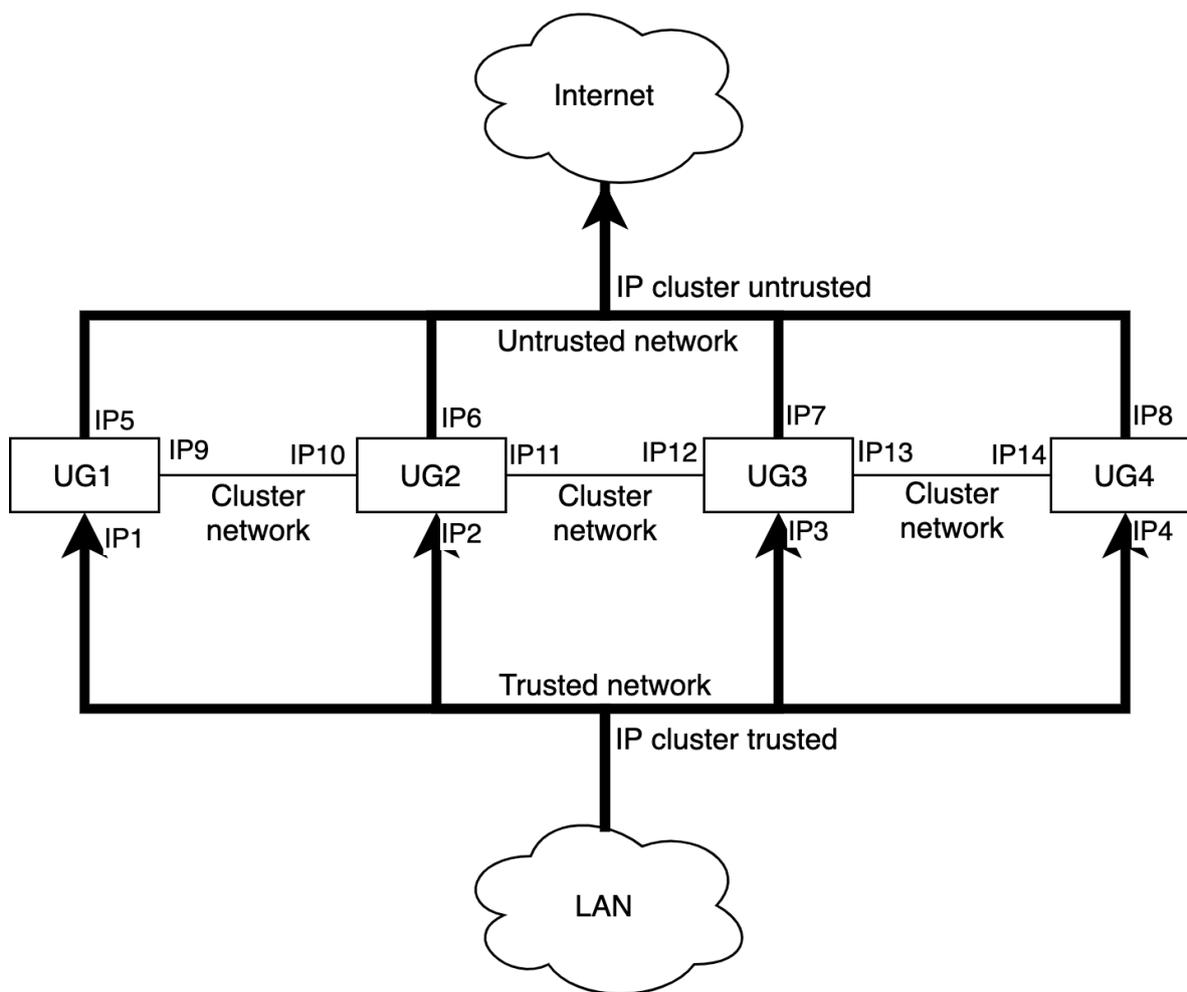
Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на запасной узел при переключении, сервера UserGate посылают служебное оповещение GARP (Gratuitous ARP), извещающий сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. В режиме Актив-Актив пакет GARP отсылается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

---

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

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

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



Отказоустойчивый кластер в режиме Актив-Актив

### **i** Примечание

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

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать кластер конфигурации	Создать кластер конфигурации, как это описано на предыдущем шаге
<b>Шаг 2.</b> Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом	В разделе <b>Зоны</b> следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес (зоны <b>Trusted</b> и <b>Untrusted</b> на диаграммах выше).

кластере	
<b>Шаг 3.</b> Создать кластер отказоустойчивости	В разделе <b>Управление устройством --&gt; Кластер отказоустойчивости</b> нажать на кнопку <b>Добавить</b> и указать параметры кластера отказоустойчивости
<b>Шаг 4.</b> Указать виртуальный IP-адрес для хостов auth.captive, logout.captive, block.captive, ftpclient.captive	Если предполагается использовать авторизацию с помощью Captive-портала, то необходимо, чтобы системные имена хостов auth.captive и logout.captive, которые используются процедурами авторизации в Captive, резолвились в IP-адрес, назначенный в качестве кластерного виртуального адреса. Более подробно эти параметры описаны в разделе <a href="#">Общие настройки</a> .

Параметры отказоустойчивого кластера:

Наименование	Описание
<b>Вкл</b>	Включение/отключение отказоустойчивого кластера
<b>Название</b>	Название отказоустойчивого кластера
<b>Описание</b>	Описание отказоустойчивого кластера
<b>Режим кластера</b>	Режим отказоустойчивого кластера: <ul style="list-style-type: none"> <li>• <b>Актив-Актив</b> - нагрузка распределяется на все узлы кластера.</li> <li>• <b>Актив-Пассив</b> - нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.</li> </ul>
<b>Синхронизировать сессии</b>	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
<b>Мультикаст идентификатор кластера</b>	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
<b>Идентификатор виртуального роутера (VRID)</b>	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
<b>Узлы</b>	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Здесь же можно назначить роль Мастер-сервера одному из выбранных узлов
<b>Виртуальные IP-адреса</b>	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера

## 4.4 Управление доступом к консоли UserGate

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

### Примечание

При первоначальной настройке UserGate создается локальный суперпользователь Admin.

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

Наименование	Описание
<b>Шаг 1.</b> Создать профиль доступа администратора	В разделе <b>Администраторы --&gt;Профили администраторов</b> нажать кнопку <b>Добавить</b> и указать необходимые настройки
<b>Шаг 2.</b> Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора	В разделе <b>Администраторы</b> нажать кнопку <b>Добавить</b> и выбрать необходимый вариант: <ul style="list-style-type: none"><li>• <b>Добавить локального администратора</b> - создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.</li><li>• <b>Добавить пользователя LDAP</b> - добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе <b>Серверы авторизации</b>. При входе в консоль администрирования необходимо указывать имя пользователя в формате <a href="#">user@domain</a>. Назначить созданный ранее профиль.</li><li>• <b>Добавить группу LDAP</b> - добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе <b>Серверы авторизации</b>. При входе в консоль администрирования необходимо указывать имя пользователя в формате <a href="#">user@domain</a>. Назначить созданный ранее профиль.</li></ul>

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
<b>Название</b>	Название профиля
<b>Описание</b>	Описание профиля
<b>Разрешения для API</b>	Список объектов, доступных для делегирования доступа при работе через программный интерфейс (API). Подробное описание объектов представлено в документации на API. В качестве доступа можно указать:

	<ul style="list-style-type: none"> <li>• Нет доступа</li> <li>• Чтение</li> <li>• Чтение и запись</li> </ul>
<b>Разрешения для веб-консоли</b>	<p>Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать:</p> <ul style="list-style-type: none"> <li>• Нет доступа</li> <li>• Чтение</li> <li>• Чтение и запись</li> </ul>
<b>Разрешения для CLI</b>	<p>Позволяет разрешить доступ к CLI. В качестве доступа можно указать:</p> <ul style="list-style-type: none"> <li>• Нет доступа</li> <li>• Чтение</li> <li>• Чтение и запись</li> </ul>

Администратор UserGate 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
<b>Шаг 1.</b> Настроить политику паролей	В разделе <b>Администраторы --&gt; Администраторы</b> нажать кнопку <b>Настроить</b>
<b>Шаг 2.</b> Заполнить необходимые поля	<p>Указать значения следующих полей:</p> <ul style="list-style-type: none"> <li>• <b>Сложный пароль</b> - 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</li> <li>• <b>Число неверных попыток аутентификации</b> - количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на <b>Время блокировки</b></li> <li>• <b>Время блокировки</b> - время, на которое блокируется учетная запись</li> </ul>

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



### 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 в разделе контроль доступа разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе **Настройка зон**.

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

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

Наименование	Описание
<b>Шаг 1.</b> Создать учетные записи дополнительных администраторов	Произвести настройку, как это описано ранее в этой главе, например, создать учетную запись администратора с именем Administrator54
<b>Шаг 2.</b> Создать или импортировать существующий сертификат типа УЦ авторизации веб-консоли	<p>Создать или импортировать существующий сертификат удостоверяющего центра (достаточно только публичного ключа) в соответствии с главой <a href="#">Управление сертификатами</a>.</p> <p>Например, для создания УЦ с помощью утилиты openssl требуется выполнить команды:</p> <pre>openssl req -x509 -subj '/C=RU/ST=Moscow/O= MyCompany /CN=ca.mycompany.com' -newkey rsa:2048 -keyout ca-key.pem -out ca.pem -nodes</pre> <pre>openssl rsa -in ca-key.pem -out ca-key.pem</pre> <p>В файле ca-key.pem будет находиться приватный ключ сертификата, в ca.pem - публичный ключ. Импортировать публичный ключ в UserGate.</p>
<b>Шаг 3.</b> Создать сертификаты для учетных записей администраторов	<p>С помощью средств сторонних утилит (например, openssl) создать сертификаты для каждого из администраторов. Необходимо, чтобы поле сертификата <b>Common name</b> в точности совпадало с именем учетной записи администратора, как она была создана в UserGate.</p> <p>Для openssl и пользователя Administrator54 команды будут следующими:</p> <pre>openssl req -subj '/C=RU/ST=Moscow/O= MyCompany /CN=Administrator54' -out admin.csr -newkey rsa:2048 -keyout admin-key.pem -nodes</pre>
<b>Шаг 4.</b> Подписать сертификаты администраторов, созданным на шаге 2 сертификатом удостоверяющего центра	<p>С помощью средств сторонних утилит (например, openssl) подписать сертификаты администраторов сертификатом удостоверяющего центра веб-консоли</p> <p>Для openssl команды будут следующими:</p> <pre>openssl x509 -req -days 9999 -CA ca.pem -CAkey ca-key.pem -set_serial 1 -in admin.csr -out admin.pem</pre> <pre>openssl pkcs12 -export -in admin.pem -inkey admin-key.pem -out admin.p12 -name 'Administrator54 client certificate'</pre> <p>Файл admin.p12 содержит подписанный сертификат администратора</p>
<b>Шаг 5.</b> Добавить подписанные	Добавить подписанные сертификаты администраторов (admin.p12 в нашем

сертификаты в ОС, с которой администраторы будут авторизоваться в веб-консоль	примере) в ОС (или в браузер Firefox, если он используется для доступа к консоли), с которой администраторы будут авторизоваться в веб-консоль. Более подробно смотрите руководство по используемой вами ОС
<b>Шаг 6.</b> Переключите режим авторизации веб-консоли в авторизацию по сертификатам x.509	В разделе <b>Настройки</b> поменяйте <b>Режим авторизации веб-консоли</b> на <b>По X.509 сертификату</b> .

### **Примечание**

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

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

## 4.5 Управление сертификатами

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

Для выполнения данных функций UserGate использует различные типы сертификатов:

Наименование	Описание
<b>SSL веб-консоли</b>	Используется для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate
<b>SSL Captive-портала</b>	Используется для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. Этот сертификат должен быть выпущен со следующими параметрами: <ul style="list-style-type: none"> <li>• Subject name - значение установленное для домена <b>Домен Auth captive-портала</b>, определенного на странице <b>Настройки</b></li> <li>• Alternative names - необходимо указать все домены, для которых используется данный сертификат, как они заданы на странице <b>Настройки</b>: <ul style="list-style-type: none"> <li>• домен Auth captive-портала</li> <li>• домен Logout captive-портала</li> <li>• домен страницы блокировки</li> <li>• домен FTP поверх HTTP</li> <li>• домен для веб-портала указанный в настройках веб-портала</li> </ul> </li> </ul> <p>По умолчанию используется подписанный с помощью сертификата инспектирование SSL сертификат, выпущенный для домена auth.captive, со следующими параметрами:</p>

	<ul style="list-style-type: none"> <li>• Subject name = auth.captive</li> </ul> <p>-Alternative names = auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive</p> <p>Если администратор не загрузил свой собственный сертификат для обслуживания этой роли, то UserGate самостоятельно в автоматическом режиме перевыпускает данный сертификат при изменении администратором одного из доменов на странице <b>Настройки</b> (домены для auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive)</p>
<b>Инспектирование SSL</b>	<p>Сертификат класса удостоверяющего центра. Он используется для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. Например, при перехвате HTTPS-трафика сайта yahoo.com оригинальный сертификат, выданный</p> <p>Subject name = yahoo.com</p> <p>Issuer name = VeriSign Class 3 Secure Server CA - G3,</p> <p>подменяется на</p> <p>Subject name = yahoo.com</p> <p>Issuer name = компания, как она указана в сертификате центра сертификации, заведенного в UserGate.</p> <p>Данный сертификат также используется для создания сертификата по умолчанию для роли SSL Captive-портала</p>
<b>SSL инспектирование (промежуточный)</b>	<p>Промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата</p>
<b>SSL инспектирование (корневой)</b>	<p>Корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата</p>
<b>Пользовательский сертификат</b>	<p>Сертификат, который назначается пользователю UserGate. Пользователь может быть, как заведен локально, так и получен из LDAP. Сертификат может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси</p>
<b>УЦ авторизации веб-консоли</b>	<p>Удостоверяющий центр авторизации администраторов для доступа к веб-консоли. Для успешной авторизации сертификат администратора должен быть подписан сертификатом этого типа</p>
<b>SAML server</b>	<p>Используется для работы UserGate с сервером SSO SAML IDP. Подробно о настройке работы UserGate с сервером авторизации SAML IDP смотрите в соответствующем разделе руководства</p>
<b>Веб-портал</b>	<p>Сертификат, используемый для веб-портала. Если данный сертификат не указан явно, то UserGate использует сертификат SSL Captive-портала, выпущенный сертификатом для инспектирования SSL. Подробно о настройке веб-портала смотрите в соответствующем разделе руководства</p>

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

UserGate поставляется с набором следующих сертификатов:

Наименование	Описание
<b>Web GUI (Default)</b>	Сертификат для SSL веб-консоли.
<b>CA (Default)</b>	Самоподписанный сертификат для инспектирования SSL.
<b>SAML (Default)</b>	Сертификат для работы с сервером SSO SAML IDP.

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

Наименование	Описание
<b>Шаг 1.</b> Создать сертификат	Нажать на кнопку <b>Создать</b> в разделе <b>Сертификаты</b>
<b>Шаг 2.</b> Заполнить необходимые поля	<p>Указать значения следующих полей:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> - название сертификата, под которым он будет отображен в списке сертификатов</li> <li>• <b>Описание</b> - описание сертификата</li> <li>• <b>Страна</b> - страна, в которой выписывается сертификат</li> <li>• <b>Область или штат</b> - область или штат, в котором выписывается сертификат</li> <li>• <b>Город</b> - город, в котором выписывается сертификат</li> <li>• <b>Название организации</b> - название организации, для которой выписывается сертификат</li> <li>• <b>Common name</b> - имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров</li> <li>• <b>E-mail</b> - e-mail вашей компании</li> </ul>
<b>Шаг 3.</b> Указать, для чего будет использован данный сертификат	<p>После создания сертификата необходимо указать его роль в UserGate. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку <b>Редактировать</b> и указать тип сертификата (SSL веб-консоли, инспектирование SSL, УЦ авторизации веб-консоли). В случае, если вы выбрали SSL веб-консоли, UserGate перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата. Сертификат инспектирования SSL начинает работать немедленно после того, как его выбрали. Более детально о инспектировании HTTPS смотрите в главе <a href="#">Инспектирование SSL</a>.</p>

UserGate 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
<b>Шаг 1.</b> Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов .
<b>Шаг 2.</b> Экспортировать сертификат	Выбрать тип экспорта: <ul style="list-style-type: none"><li>• <b>Экспорт сертификата</b> - экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом читайте в приложении <a href="#">Приложение 1. Установка сертификата локального удостоверяющего центра</a>.</li><li>• <b>Экспорт CSR</b> - экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.</li></ul>



#### Примечание

Рекомендуется сохранять сертификат для возможности его последующего восстановления.



#### Примечание

В целях безопасности UserGate не разрешает экспорт приватных ключей сертификатов.



#### Примечание

Пользователи могут скачать себе для установки сертификат инспектирования SSL с UserGate по прямой ссылке: **Ошибка! Недопустимый объект гиперссылки.** UserGate\_IP:8002/cps/ca

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

Наименование	Описание
<b>Шаг 1.</b> Начать импорт	Нажать на кнопку <b>Импорт</b>

**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

### 4.5.1 Использование корпоративного УЦ для создания сертификата инспектирования SSL

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

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

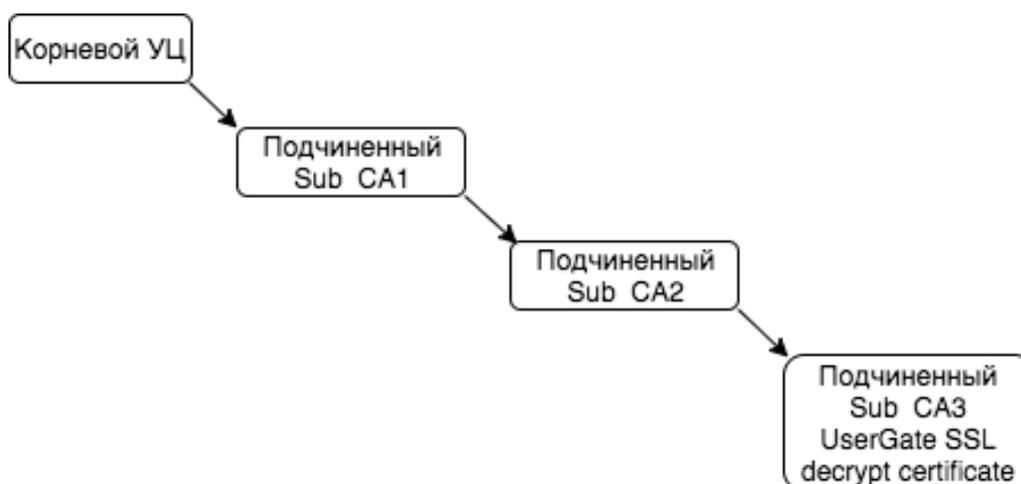


Рисунок Пример структуры корпоративного УЦ

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

#### **Примечание**

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

Для выполнения этой задачи следует выполнить следующие шаги:

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

## 4.6 Интерфейс командной строки (CLI)

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

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

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

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

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

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

Наименование	Описание
<b>Шаг 1.</b> Подключиться к UserGate	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate
<b>Шаг 2.</b> 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
<b>Шаг 3.</b> Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm

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

Наименование	Описание
<b>Шаг 1.</b> 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
<b>Шаг 2.</b> Запустить SSH-терминал	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UserGate, в качестве порта подключения - 2200, в качестве имени пользователя - имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так:

	<code>ssh Admin@IP UserGate -p 2200</code>
<b>Шаг 3.</b> Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm

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

### help command

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

### help iface

Полный список команд:

Наименование	Описание
<b>help</b>	Показывает список доступных команд.
<b>exit</b> <b>quit</b> <b>Ctrl+D</b>	Выйти из CLI.
<b>cache ldap-clear</b>	Очистка кэша LDAP-записей.
<b>code-change-control</b>	<p>Набор команд для просмотра и настройки параметров защиты исполняемого кода продукта от потенциального несанкционированного изменения. Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate.</p> <p><b>code-change-control show</b> - показывает текущий режим работы. По умолчанию отслеживание несанкционированных изменений исполняемого кода отключено.</p> <p><b>code-change-control set log</b> - активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требуется задания пароля, который потребуется в случае изменения режима отслеживания.</p> <p><b>code-change-control set block</b> - активирует режим отслеживания несанкционированных изменений исполняемого кода. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.</p> <p><b>code-change-control set off</b> - отключает режим отслеживания несанкционированных изменений исполняемого кода. Требуется указания пароля, который был задан при активации режима отслеживания исполняемого кода.</p>

<b>config-change-control</b>	<p>Набор команд для просмотра и настройки параметров защиты конфигурации (настроек) продукта от изменения. Перед активацией защиты конфигурации администратор производит настройку продукта в соответствии с требованиями организации, после чего "замораживает" настройки (режим <b>log</b> или <b>block</b>). Любое изменение настроек через веб-интерфейс, CLI или другими способами будет приводить к журналированию и/или блокировке транзитного трафика, в зависимости от выбранного режима.</p> <p>Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate.</p> <p><b>config-change-control show</b> - показывает текущий режим работы. По умолчанию отслеживание изменений конфигурации отключено.</p> <p><b>config-change-control set log</b> - активирует режим отслеживания изменений конфигурации. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требуется задания пароля, который потребуется в случае изменения режима отслеживания.</p> <p><b>config-change-control set block</b> - активирует режим отслеживания изменений конфигурации. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для отключения созданного правила межсетевого экрана необходимо сбросить состояние блокировки с помощью следующей команды:</p> <p><b>config-change-control set off</b> - отключает режим отслеживания изменений конфигурации. Требуется указания пароля, который был задан при активации режима отслеживания конфигурации.</p>
<b>date</b>	<p>Посмотреть текущее время на сервере.</p>
<b>device</b>	<p>Набор команд для изменения параметров устройства.</p> <p><b>device passwd</b> - позволяет сменить пароль пользователю, залогиненному в CLI-консоль.</p> <p><b>device config -list</b> - показывает список доступных опций для настройки.</p> <p><b>device config -get</b> - посмотреть текущее значение параметра.</p> <p><b>device config -set</b> - изменить значение параметра.</p> <p>Список доступных параметров:</p> <p><b>module_l7_enabled</b> - включение/отключение загрузки модуля L7. По умолчанию модуль загружен.</p> <p><b>module_idps_enabled</b> - включение/отключение загрузки модуля idps. По умолчанию модуль загружен.</p> <p><b>module_h323_enabled</b> - включение/отключение загрузки модуля h323. По умолчанию модуль выгружен.</p> <p><b>module_sip_enabled</b> - включение/отключение загрузки модуля sip. По умолчанию модуль выгружен.</p> <p><b>module_sunrpc_enabled</b> - включение/отключение загрузки модуля sunrpc. По умолчанию модуль выгружен.</p> <p><b>module_ftp_alg_enabled</b> - включение/отключение загрузки модуля ftp. По умолчанию модуль выгружен.</p> <p><b>ha_checker_ping</b> - включение дополнительной проверки состояния кластера отказоустойчивости.</p>

	<p>Узел будет переведен в состояние Slave если ping до указанного в команде хоста будет не успешен. Для включения проверки необходимо использовать синтаксис:</p> <pre>device config -set ha_checker_ping true; ip</pre> <p>для отключения проверки</p> <pre>device config -set ha_checker_ping false</pre> <p><b>ha_checker_master</b> - включение дополнительной проверки состояния кластера отказоустойчивости. Узел будет переведен в состояние Slave, если запрос XMLRPC до указанного в команде сервера UserGate будет не успешен. Запрос успешен только в том случае, если сервер UserGate доступен и является Master-сервером кластере. Как правило такая проверка необходима для синхронизации состояний серверов в двух различных кластерах.</p> <p>Для включения проверки необходимо использовать синтаксис:</p> <pre>device config - set ha_checker_master true; i p</pre> <p>для отключения проверки</p> <pre>device config -set ha_checker_master false</pre> <p>На сервере UserGate, куда посылается проверочный запрос, должен быть разрешен сервис XMLRPC на зоне, на интерфейсы которой приходит данный запрос.</p> <p><b>ha_auth_type</b> - включение подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости. Для включения подписи необходимо использовать команду:</p> <pre>device config -set ha_auth_type ah</pre> <p>для отключения проверки</p> <pre>device config -set ha_auth_type pass</pre>
<b>gateway</b>	Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации.
<b>iface</b>	Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации.
<b>license</b>	Посмотреть информацию о лицензии.
<b>netcheck</b>	<p>Проверить доступность стороннего HTTP/HTTPS-сервера.</p> <p><b>netcheck [-t TIMEOUT] [-d] URL</b></p> <p>Опции:</p> <ul style="list-style-type: none"> <li>-t – максимальный таймаут ожидания ответа от веб-сервера</li> <li>-d – запросить содержание сайта. По умолчанию запрашиваются только заголовки.</li> </ul>
<b>node</b>	Набор команд для просмотра и настройки узлов кластера. Смотрите node help для детальной информации.
<b>nslookup</b>	Выполнить определение IP-адреса по имени хоста.

<b>ping</b>	Выполнить ping определенного хоста.
<b>proxy</b>	<p>Набор команд для просмотра и настройки параметров прокси-сервера. Позволяет настроить такие параметры, как добавление заголовков HTTP - via и forwarded, а также настройки таймаутов на подключение к сайтам и на загрузку контента:</p> <ul style="list-style-type: none"> <li>• add_via_enabled – добавлять http заголовок via. По умолчанию отключено.</li> <li>• add_forwarded_enabled – добавлять http заголовок forwarded. По умолчанию отключено.</li> <li>• http_connection_timeout – время ожидания, выделяемое на подключение http. По умолчанию - 20 секунд.</li> <li>• http_loading_timeout – время ожидания, выделяемое на загрузку контента http. По умолчанию - 60 секунд.</li> <li>• proxy_host_rfc - разрешить использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. По умолчанию установлено значение strict (соблюдать RFC).</li> <li>• fmode_enabled (boolean) - включает режим ускорения загрузки контента. Может быть несовместим с работой некоторых сайтов. По умолчанию отключен.</li> <li>• icap_wait_timeout - время в секундах, которое сервер UserGate ждет ответа от ICAP-сервера. Если ответ сервера не был получен в заданный промежуток времени, то в случае, если действие правила <b>Переслать и игнорировать</b>, UserGate отправит данные пользователю без модификации, если же действие правила <b>Переслать</b>, UserGate не отдаст данные пользователю. Значение по умолчанию - 10 секунд.</li> <li>• smode_enabled (boolean) – включает режим SYN Proxy. По умолчанию включен.</li> <li>• legacy_ssl_enabled (boolean) – отключает поддержку дешифрования протокола SSL TLSv1.3. При включении данного режима UserGate поддерживает работу протоколов TLSv1.0-TLSv1.2. Если режим отключен, то поддерживается работа только TLSv1.0-TLSv1.3. По умолчанию отключен.</li> </ul> <p>Рекомендуется не изменять значения по умолчанию. Смотрите proxy help для детальной информации.</p>
<b>radmin</b>	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate.
<b>radmin_e</b>	<p>Включить или отключить удаленный доступ к серверу для технической поддержки UserGate, в случаях, когда сервер UserGate завис.</p> <p>В случаях, когда произошла проблема с ядром UserGate, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации UserGate. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде <a href="#">Admin@emergency</a>, в качестве пароля - пароль корневого администратора.</p>
<b>reboot</b>	Перезагрузить сервер UserGate.
<b>route</b>	Создать, изменить, удалить маршрут.
<b>shutdown</b>	Выключить сервер UserGate.
<b>telemetry</b>	Набор команд для просмотра и настройки режима работы телеметрии. Телеметрия позволяет отправлять разработчику анонимную статистику, такую как, популярность веб-сайтов, веб-сайты с неизвестной категорией, вирусные атаки, события COB, активность малваре. Данные телеметрии

	<p>имеют вид обезличенных данных и не содержат персональную информацию. Отправка телеметрии активирована по умолчанию.</p> <p>telemetry show – показать текущий режим</p> <p>telemetry set -enabled true – активировать телеметрию</p> <p>telemetry set -enabled false – отключить отсылку телеметрической информации.</p>
<b>traceroute</b>	Выполнить трассировку соединения до определенного хоста.
<b>usersession</b>	<p>Команда для сброса авторизации указанного пользователя.</p> <p><b>usersession terminate -ipv4 IP_ADDRESS</b> – сбрасывает авторизацию для указанного IP_ADDRESS.</p>
<b>webaccess</b>	Набор команд для просмотра режима авторизации веб-консоли. Позволяет вернуть режим <b>По имени и паролю</b> при невозможности авторизоваться с помощью сертификатов.
<b>zone</b>	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

## 4.7 Системные утилиты

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

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

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

<b>5. Memory test</b>	Запуск проверки оперативной памяти устройства.
-----------------------	--

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

Наименование	Описание
<b>Check filesystems</b>	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
<b>Clear logs</b>	Очистка диагностических журналов для освобождения пространства на системном разделе. Журналы UserGate не очищаются (журналы веб-доступа, трафика, событий, COB и т.п.).
<b>Export logs</b>	Выгрузка диагностических журналов на внешний USB носитель. Все данные на внешнем носителе будут удалены.
<b>Expand log partition</b>	Увеличение раздела для журналов на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate. Данные и настройки UserGate не сбрасываются.
<b>Backup full</b>	Создать полную копию диска UserGate на внешний USB носитель. Все данные на внешнем носителе будут удалены.
<b>Backup system only</b>	Создать копию системного раздела UserGate, исключая журналы (журналы веб-доступа, трафика, событий, COB и т.п.) на внешний USB носитель. Все данные на внешнем носителе будут удалены.
<b>Restore from backup</b>	Восстановление UserGate с внешнего USB носителя.
<b>Update from USB</b>	Установка обновления ПО UserGate с внешнего USB носителя. Обновление должно быть скопировано в корень съемного диска, диск должен иметь формат NTFS или FAT32.
<b>Refresh NIC names</b>	Упорядочивание имен сетевых портов в необходимом порядке. Упорядочивание производится в соответствии с номером порта на шине PCI. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UserGate не сбрасываются.
<b>Factory reset</b>	Сброс состояния UserGate к первоначальному состоянию системы. Все данные и настройки будут утеряны.
<b>Exit</b>	Выход и перезагрузка устройства.

## 5 НАСТРОЙКА СЕТИ

В данном разделе описаны основные сетевые настройки UserGate.

### 5.1 Настройка зон

Зона в UserGate - это логическое объединение сетевых интерфейсов. Политики безопасности UserGate используют зоны интерфейсов, а не непосредственно интерфейсы. Это дает необходимую гибкость политикам безопасности, а также существенно упрощает управление отказоустойчивым кластером. Зоны одинаковы на всех узлах кластера, то есть данная настройка является глобальной для кластера.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов, подключенных к сети партнера и т.п.

По умолчанию UserGate поставляется со следующими зонами:

Наименование	Описание
<b>Management</b>	Зона для подключения доверенных сетей, из которых разрешено управление UserGate
<b>Trusted</b>	Зона для подключения доверенных сетей, например, LAN-сетей
<b>Untrusted</b>	Зона для интерфейсов, подключенных к недоверенным сетям, например, к интернету
<b>DMZ</b>	Зона для интерфейсов, подключенных к сети DMZ
<b>Cluster</b>	Зона для интерфейсов, используемых для работы кластера
<b>VPN for Site-to-Site</b>	Зона, в которую помещаются все клиенты типа Офис-Офис, подключаемые к UserGate по VPN
<b>VPN for remote access</b>	Зона, в которую помещаются все мобильные пользователи, подключаемые к UserGate по VPN

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



#### Примечание

Можно создать не более 15 зон.

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1. Создать зону</b>	Нажать на кнопку <b>Добавить</b> и дать название зоне

<p><b>Шаг 2.</b> Настроить параметры защиты зоны от DoS (опционально)</p>	<p>Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP:</p> <ul style="list-style-type: none"> <li>• <b>Агрегировать</b> - если установлено, то считаются все пакеты, входящие в интерфейсы данной зоны. Если не установлено, то считаются пакеты отдельно для каждого IP-адреса.</li> <li>• <b>Порог уведомления</b> - при превышении количества запросов над указанным значением происходит запись события в системный журнал.</li> <li>• <b>Порог отбрасывания пакетов</b> - при превышении количества запросов над указанным значением UserGate начинает отбрасывать пакеты и записывает данное событие в системный журнал.</li> </ul> <p>Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов - 600 запросов в секунду. Рекомендуется включать защиту от флуда на всех интерфейсах, за исключением интерфейсов зоны <b>Cluster</b>.</p> <p>Необходимо увеличить пороговое значение отбрасывания пакетов для протокола UDP, если через интерфейсы зоны проходит трафик таких сервисов, как IP-телефония или L2TP VPN.</p> <p><b>Исключения защиты от DoS</b> - позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для сервиса IP-телефонии, так как он шлет большое количество UDP-пакетов.</p> <p>Важно! UserGate позволят произвести более гранулированную защиту от DoS атак. Для получения дополнительной информации обратитесь в раздел <a href="#">Защита от DoS атак</a>.</p>
<p><b>Шаг 3.</b> Настроить параметры контроля доступа зоны (опционально)</p>	<p>Указать предоставляемые UserGate сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы.</p> <p>Сервисы:</p> <ul style="list-style-type: none"> <li>• <b>Ping</b> - позволяет пинговать UserGate</li> <li>• <b>SNMP</b> - доступ к UserGate по протоколу SNMP (UDP 161)</li> <li>• <b>Captive-портал</b> и <b>страница блокировки</b> - необходимы для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002)</li> <li>• <b>XML-RPC</b> для управления - позволяет управлять продуктом по API (TCP 4040)</li> <li>• <b>Кластер</b> - сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100)</li> <li>• <b>VRRP</b> - сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112)</li> <li>• <b>Консоль администрирования</b> - доступ к веб-консоли управления (TCP 8001)</li> <li>• <b>DNS</b> - доступ к сервису DNS-прокси (TCP 53, UDP 53)</li> <li>• <b>HTTP(S)-прокси</b> - доступ к сервису HTTP(S)-прокси (TCP 8090)</li> <li>• <b>Агент авторизации</b> - доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813)</li> <li>• <b>SMTP(S)-прокси</b> - сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел <a href="#">Защита почтового трафика</a>.</li> <li>• <b>POP3(S)-прокси</b> - сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел <a href="#">Защита почтового трафика</a>.</li> <li>• <b>CLI по SSH</b> - доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>VPN</b> - доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500)</li> <li>• <b>SCADA</b> - сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. Более подробно смотрите раздел <a href="#">Правила АСУ ТП</a>.</li> <li>• <b>Reverse-прокси</b> – сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. Более подробно смотрите раздел <a href="#">Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси</a>.</li> <li>• <b>Web-портал</b>– сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. Более подробно смотрите раздел <a href="#">Веб-портал</a>.</li> <li>• <b>Log Analyzer</b> – сервис для подключения к анализатору журналов Log Analyzer.</li> <li>• <b>OSPF</b> – сервис динамической маршрутизации OSPF. Более подробно смотрите раздел <a href="#">OSPF</a>.</li> <li>• <b>BGP</b>– сервис динамической маршрутизации BGP. Более подробно смотрите раздел <a href="#">BGP</a>.</li> <li>• <b>NTP service</b> - разрешает доступ к сервису точного времени, запущенному на сервере UserGate.</li> </ul>
<p><b>Шаг 4.</b> Настроить параметры защиты от IP-спуфинг атак (опционально)</p>	<p>Атаки на основе IP-спуфинга позволяют передать пакет из внешней сети, например, из <b>Untrusted</b>, во внутреннюю, например, в <b>Trusted</b>. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес внутренней сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес.</p> <p>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.</p> <p>С помощью галочки <b>Инвертировать</b> 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, для зоны Untrusted можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 и включить опцию <b>Инвертировать</b>.</p>

## 5.2 Настройка интерфейсов

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN-интерфейсы. Раздел отображает все интерфейсы каждого узла кластера. Настройки интерфейсов специфичны для каждого из узлов, то есть не глобальны.

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

- Включить или отключить интерфейс
- Указать тип интерфейса - Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа.
- Назначить зону интерфейсу
- Назначить профиль Netflow для отправки статистических данных на Netflow коллектор
- 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

- Настроить работу DHCP-релея на выбранном интерфейсе. Для этого необходимо включить DHCP-релей, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

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

- VLAN.
- Бонд.
- Мост.
- PPPoE.
- VPN.
- Туннель.

### 5.2.1 Создание интерфейса VLAN

С помощью кнопки **Добавить VLAN** администратор может создавать сабинтерфейсы. При создании VLAN необходимо указать следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает VLAN
<b>Название</b>	Название VLAN. Название присваивается автоматически на основе имени физического порта и тега VLAN.
<b>Описание</b>	Оptionальное описание интерфейса.
<b>Тип интерфейса</b>	Указать тип интерфейса - Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа.
<b>Тег VLAN</b>	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов.
<b>Имя узла</b>	Имя узла в кластере, на котором создается данный VLAN.
<b>Интерфейс</b>	Физический интерфейс, на котором создается VLAN.
<b>Зона</b>	Зона, к которой принадлежит VLAN.
<b>Профиль Netflow</b>	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе <a href="#">Профили Netflow</a> .
<b>Сеть</b>	Способ присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP
<b>DHCP-релей</b>	Настройка работы DHCP-релея на бонд-интерфейсе. Необходимо включить DHCP-релей, указать в поле <b>Адрес UserGate</b> IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

## 5.2.2 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
<b>Вкл</b>	Включает бонд
<b>Название</b>	Название бонда
<b>Имя узла</b>	Узел кластера UserGate, на котором будет создан бонд
<b>Зона</b>	Зона, к которой принадлежит бонд
<b>Профиль Netflow</b>	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе <a href="#">Профили Netflow</a> .
<b>Интерфейсы</b>	Один или более интерфейсов, которые будут использованы для построения бонда
<b>Режим</b>	<p>Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть:</p> <ul style="list-style-type: none"><li>• <b>Round robin.</b> Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости</li><li>• <b>Active backup.</b> 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</li><li>• <b>XOR.</b> 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</li><li>• <b>Broadcast.</b> Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости</li><li>• <b>IEEE 802.3ad</b> - 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</li><li>• <b>Adaptive transmit load balancing.</b> 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</li><li>• <b>Adaptive load balancing.</b> Включает в себя предыдущую политику плюс осуществляет</li></ul>

	<p>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</p>
<b>MII monitoring period (мсек)</b>	<p>Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию - 0 - отключает MII-мониторинг</p>
<b>Down delay (мсек)</b>	<p>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</p>
<b>Up delay (мсек)</b>	<p>Задаёт 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</p>
<b>LACP rate</b>	<p>Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения:</p> <ul style="list-style-type: none"> <li>• <b>Slow</b> - запрос партнера на передачу LACPDU-пакетов каждые 30 секунд</li> <li>• <b>Fast</b> - запрос партнера на передачу LACPDU-пакетов каждую 1 секунду</li> </ul>
<b>Failover MAC</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Отключено</b> - устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения</li> <li>• <b>Active</b> - 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</li> <li>• <b>Follow</b> - 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</li> </ul>
<b>Xmit hash policy</b>	<p>Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:</p> <ul style="list-style-type: none"> <li>• <b>Layer 2</b> - 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</li> <li>• <b>Layer 2+3</b> - использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Layer 3+4</b> - 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 прийти до получателя не в том порядке, так как отправляются через разные интерфейсы</li> </ul>
<b>Сеть</b>	Способ присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP
<b>DHCP-релей</b>	Настройка работы DHCP-релея на бонд-интерфейсе. Необходимо включить DHCP-релей, указать в поле <b>Адрес UserGate</b> IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

### 5.2.3 Создание моста (bridge)

Сетевой мост работает на канальном уровне сетевой модели OSI (L2), при получении из сети [кадра](#) сверяет [MAC-адрес](#) последнего и, если он не принадлежит данной подсети, передает (транслирует) кадр дальше в тот сегмент, которому предназначался данный кадр; если кадр принадлежит данной подсети, мост ничего не делает.

Интерфейс мост можно использовать в UserGate аналогично обычному интерфейсу. Кроме этого, через мост можно настроить фильтрацию передаваемого контента уровне L2 без внесения изменений в сетевую инфраструктуру компании. Простейшая схема использования UserGate в качестве решения, обеспечивающего контентную фильтрацию на уровне L2, выглядит следующим образом:

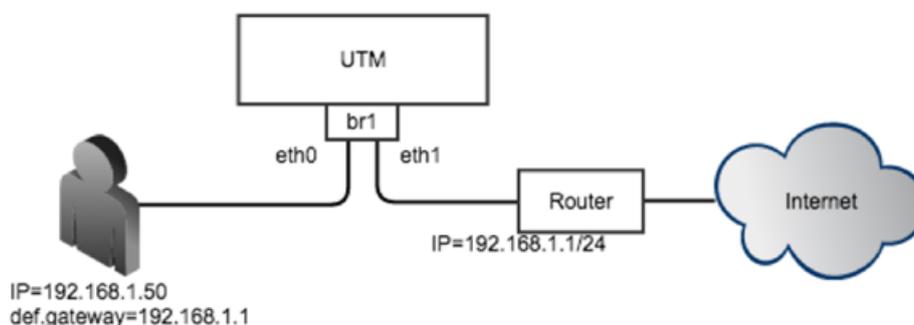


Рисунок Использование моста

При создании моста можно указать режим его работы - Layer 2 или Layer 3.

При выборе режима Layer 2 создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Контентной фильтрации и Mail security.

При выборе режима Layer 3 создаваемому мосту необходимо назначить IP-адрес и указать маршруты в сети, подключенные к интерфейсам моста. В данном режиме могут быть использованы все механизмы фильтрации, доступные в UserGate.

Если мост создается в ПАК UserGate, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить 2 интерфейса в байпас-мост. Байпас-мост автоматически переключает два выбранных интерфейса в режим байпас (закорачивает их, пропуская весь трафик мимо UserGate) в случаях если:

- Электропитание ПАК UserGate отключено
- Система внутренней диагностики обнаружила проблему в работе ПО UserGate.

Более подробно о сетевых интерфейсах, поддерживающих режим байпас смотрите в спецификации на оборудование ПАК UserGate.

С помощью кнопки **Добавить мост** администратор может объединить несколько физических интерфейсов в новый тип интерфейса - мост. Необходимо указать следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает интерфейс мост
<b>Название</b>	Название интерфейса
<b>Имя узла</b>	Узел кластера UserGate, на котором создать интерфейс мост
<b>Тип интерфейса</b>	Указать тип интерфейса - Layer 3 или Layer 2.
<b>Зона</b>	Зона, к которой принадлежит интерфейс мост
<b>Профиль Netflow</b>	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе <a href="#">Профили Netflow</a> .
<b>Интерфейсы моста</b>	Два интерфейса, которые будут использованы для построения моста
<b>Интерфейсы байпас моста</b>	Пара интерфейсов, которые можно использовать для построения байпас моста. Требуется поддержка оборудования ПАК UserGate.
<b>STP (Spanning Tree Protocol)</b>	Включает использование STP для защиты сети от петель
<b>Forward delay</b>	Задержка перед переключением моста в активный режим (Forwarding), в случае, если включен STP
<b>Maximum age</b>	Время, по истечении которого STP-соединение считается потерянным
<b>Сеть</b>	Способ присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP
<b>DHCP-релей</b>	Настройка работы DHCP-релея на бонд-интерфейсе. Необходимо включить DHCP-релей, указать в поле <b>Адрес UserGate</b> IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

## 5.2.4 Интерфейс PPPOE

PPPoE (Point-to-point protocol over Ethernet) – сетевой протокол канального уровня передачи кадров PPP через Ethernet. С помощью кнопки **Добавить Интерфейс PPPOE** администратор может создать PPPOE интерфейс. При создании необходимо указать следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает интерфейс PPPOE.
<b>Имя узла</b>	Узел кластера UserGate, на котором создать интерфейс PPPOE.
<b>Интерфейс</b>	Указать интерфейс, на котором будет создаваться интерфейс PPPOE.
<b>Профиль Netflow</b>	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе <a href="#">Профили Netflow</a> .
<b>Зона</b>	Зона, к которой принадлежит интерфейс PPPOE.
<b>MTU</b>	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet.
<b>Логин</b>	Имя пользователя для соединения PPPOE.
<b>Пароль</b>	Пароль пользователя для соединения PPPOE.
<b>Переподключаться автоматически</b>	Включает переподключение соединения при обрыве связи.
<b>Интервал между попытками подключения (сек.)</b>	Интервал времени в секундах после разрыва соединения перед повторным запуском.
<b>Маршрут по умолчанию</b>	Устанавливает интерфейс PPPOE в качестве маршрута по умолчанию.
<b>Интервал проверки соединения (сек.)</b>	Интервал проверки соединения
<b>Количество неуспешных проверок</b>	Количество неуспешных проверок соединения, после которого UserGate считает, что соединение отсутствует и разрывает его.
<b>Использовать DNS-сервер провайдера</b>	Если опция включена, то UserGate использует DNS-сервера, выданные провайдером.
<b>Количество попыток подключения</b>	Количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены.

## 5.2.5 Интерфейс VPN

VPN-интерфейс – это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

В разделе **Сеть --> Интерфейсы** нажмите кнопку **Добавить**, и выберите **Добавить VPN**. Задайте следующие параметры:

Наименование	Описание
<b>Название</b>	Название интерфейса, должно быть в виде tunnelN, где N – это порядковый номер VPN-интерфейса.
<b>Описание</b>	Описание интерфейса.
<b>Зона</b>	Зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к серверу UserGate будут так же помещены в эту зону.
<b>Профиль Netflow</b>	Профиль Netflow, используемый для данного интерфейса. Не обязательный параметр.
<b>Режим</b>	Тип присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN, то необходимо использовать статический IP-адрес. Для использования интерфейса, используемого в роли клиента, необходимо выбрать Динамический режим.
<b>MTU</b>	Размер MTU для выбранного интерфейса.

По умолчанию в системе уже созданы 3 VPN-интерфейса:

- tunnel1, который рекомендовано использовать для Remote access VPN.
- tunnel2, который рекомендовано использовать для серверной части Site-to-Site VPN.
- tunnel3, который рекомендовано использовать для клиентской части Site-to-Site VPN.

## 5.2.6 Интерфейс туннель

Интерфейс туннель – это виртуальный сетевой адаптер, который может использоваться для создания соединения точка-точка через IP-сеть. Поддерживаются следующие типы туннельных интерфейсов:

- GRE - протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение – инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP - 47.
- IPsec - это протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP пакета в другой IP пакет, это добавление внешнего заголовка с Source IP - точкой входа в туннель, и Destination - точкой выхода из туннеля.
- VXLAN - это протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789.

Для создания туннельного интерфейса в разделе **Сеть --> Интерфейсы** нажмите кнопку **Добавить**, и выберите **Добавить туннель**. Задайте следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включение или выключение данного интерфейса.
<b>Название</b>	Название интерфейса, должно быть в виде greN, где N – это порядковый номер туннельного интерфейса.
<b>Описание</b>	Описание интерфейса.
<b>Зона</b>	Зона, к которой будет относиться данный интерфейс.
<b>Режим</b>	Режим работы туннеля - GRE, IPIP, VXLAN.
<b>MTU</b>	Размер MTU для выбранного интерфейса.
<b>Локальный IP</b>	Локальный адрес point-to-point интерфейса.
<b>Удаленный IP</b>	Удаленный адрес point-to-point интерфейса.
<b>IP интерфейса</b>	IP-адрес, назначенный туннельному интерфейсу.
<b>VXLAN ID</b>	Идентификатор VXLAN. Только для типа туннеля VXLAN.

## 5.2.7 Настройка Netflow

Netflow - сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу Netflow требуются следующие компоненты:

- Сенсор - собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор - получает от сенсора данные и помещает их в хранилище.
- Анализатор - анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты (часто в виде графиков).

Сервер UserGate может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс UserGate, необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать профиль Netflow	В разделе <b>Библиотеки --&gt; Профили Netflow</b> нажать на кнопку <b>Добавить</b> и создать профиль Netflow. Подробнее о профиле Netflow смотрите раздел <a href="#">Профили Netflow</a> .
<b>Шаг 2.</b> Назначить созданный профиль Netflow сетевому интерфейсу, на котором необходимо	В разделе <b>Сеть --&gt; Интерфейсы</b> в настройках конкретного

## 5.3 Настройка шлюзов

Для подключения UserGate к интернету необходимо указать IP-адрес одного или нескольких шлюзов. Если для подключения к интернету используется несколько провайдеров, то необходимо указать несколько шлюзов. Настройка шлюза уникальна для каждого из узлов кластера.

Пример настройки сети с двумя провайдерами:

- Интерфейс eth1 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 eth2 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
<b>Балансировка трафика между шлюзами</b>	<p>Установить флажок <b>Балансировка</b> и указать <b>Вес</b> 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).</p> <p>При распределении трафика между шлюзами с разными весами происходит:</p> <ol style="list-style-type: none"> <li>1. Вычисление хэша от адресов источника и назначения.</li> <li>2. Выбор шлюза.</li> </ol> <p>Трафик распределяется с учётом весов. Пусть настроены 2 шлюза:</p> <ul style="list-style-type: none"> <li>• <b>n1, n2</b> – сессии, проходящие через шлюзы.</li> <li>• <b>w1, w2</b> – веса шлюзов.</li> </ul> <p>Тогда сессии между шлюзами будут распределяться согласно <math>n1/w1 = n2/w2</math>.</p>
<b>Основной шлюз с переключением на запасной</b>	<p>Выбрать один из шлюзов в качестве основного и настроить <b>Проверку сети</b>, нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет (с помощью ping) 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.</p> <p>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.</p>

Состояние шлюза (доступен - зеленый, не доступен - красный) определяется следующим образом:

Наименование	Описание
<b>Проверка сети отключена</b>	Шлюз считается доступным, если UserGate может получить его MAC-адрес с помощью ARP-запроса. Проверка наличия доступа в интернет через этот шлюз не производится.

	Если MAC-адрес шлюза не может быть определен, шлюз считается недоступным.
<b>Проверка сети включена</b>	<p>Шлюз считается доступным, если:</p> <ul style="list-style-type: none"> <li>• UserGate может получить его MAC-адрес с помощью ARP-запроса.</li> <li>• Проверка наличия доступа в интернет через этот шлюз завершилась успешно.</li> </ul> <p>В противном случае шлюз считается недоступным.</p>

## 5.4 Настройка DHCP

Служба DHCP (Dynamic Host Configuration Protocol) позволяет автоматизировать процесс выдачи сетевых настроек клиентам в локальной сети. В сети с DHCP-сервером каждому сетевому устройству можно динамически назначать IP-адрес, адрес шлюза, DNS.

UserGate может также выступать в качестве DHCP-релея, обеспечивая передачу DHCP-запросов от клиентов, находящихся в различных сетях, на центральный DHCP-сервер. Более подробно о настройке DHCP-релея можно посмотреть в разделе **Настройка интерфейсов**.

В UserGate можно создать несколько диапазонов адресов для выдачи по DHCP. DHCP работает на каждом узле отказоустойчивого кластера независимо. Для обеспечения отказоустойчивости сервиса DHCP в кластере необходимо настроить DHCP на обоих узлах, указав непересекающиеся диапазоны IP-адресов.

Для создания диапазона DHCP необходимо нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
<b>Включен</b>	Включает или отключает использование данного диапазона DHCP
<b>Узел</b>	Узел кластера, на котором создается данный диапазон
<b>Интерфейс</b>	Интерфейс сервера, на котором будут раздаваться IP-адреса из создаваемого диапазона
<b>Диапазон IP</b>	Диапазон IP-адресов, выдаваемый клиентам DHCP
<b>Маска</b>	Маска подсети, выдаваемая клиентам DHCP
<b>Время аренды</b>	Время в секундах, на которое выдаются IP-адреса
<b>Домен</b>	Название домена, выдаваемое клиентам DHCP
<b>Шлюз</b>	IP-адрес шлюза, выдаваемый клиентам DHCP
<b>Серверы имен</b>	IP-адрес DNS-серверов, выдаваемых клиентам DHCP.
<b>Зарезервированные адреса</b>	MAC-адреса и сопоставленные с ними IP-адреса

<b>Игнорируемые MAC</b>	Список MAC-адресов, игнорируемых DHCP-сервером
<b>DHCP PXE boot</b>	Адрес сервера и имя загрузочного файла, передаваемого на запрос PXE boot
<b>DHCP опции</b>	Номер опции и ее значение.

Выданные IP-адреса отображаются в панели **Арендованные адреса**. Администратор может освободить любой выданный адрес, выделив адрес и нажав на кнопку **Освободить**.

## 5.5 Настройка DNS

Данный раздел содержит настройки сервисов DNS и DNS-прокси.

Для корректной работы продукта необходимо, чтобы UserGate мог разрешать доменные имена в IP-адреса. Укажите корректные IP-адреса серверов DNS в настройке **Системные DNS-серверы**.

Сервис DNS-прокси позволяет перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора.

Настройки DNS-прокси:

Наименование	Описание
<b>Кэширование DNS</b>	Включает или отключает кэширование ответов DNS. Рекомендуется оставить включенным для ускорения обслуживания клиентов
<b>DNS-фильтрация</b>	Включает или отключает фильтрацию DNS-запросов. Для работы фильтрации необходимо приобрести лицензию на модуль ATP
<b>Рекурсивные DNS-запросы</b>	Разрешает или запрещает серверу осуществлять рекурсивные DNS-запросы. Рекомендуется оставить эту опцию включенной
<b>Максимальный TTL для DNS-записей</b>	Устанавливает максимально возможное время жизни для записей DNS
<b>Лимит количества DNS-запросов в секунду на пользователя</b>	Устанавливает ограничение на количество DNS-запросов в секунду для каждого пользователя. Запросы, превышающие данный параметр, будут отброшены. Значение по умолчанию - 100 запросов в секунду. Не рекомендуется ставить большие значения для данного параметра, поскольку DNS-флуд (DNS DoS attacks) является довольно частой причиной отказа обслуживания DNS-серверов
<b>Только A и AAAA DNS-записи для не идентифицированных пользователей (защита от VPN поверх DNS)</b>	Если защита включена, то UserGate отвечает только на запросы на записи A и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS

С помощью правил DNS-прокси можно указать серверы DNS, на которые пересылаются запросы на определенные домены. Данная опция может быть полезна в случае, если внутри компании используется

локальный домен, не имеющий связи с интернетом и использующийся для внутренних нужд компании, например, домен Active Directory.

Чтобы создать правило DNS-прокси, необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Добавить правило	Нажать на кнопку <b>Добавить</b> , задать <b>Название</b> и <b>Описание</b> (опционально)
<b>Шаг 2.</b> Указать список доменов	Задать список доменов, которые необходимо перенаправлять, например, localdomain.local. Допускается использование "*" для указания шаблона доменов
<b>Шаг 3.</b> Указать DNS-серверы	Задать список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены

Кроме этого, с помощью DNS-прокси можно задавать статические записи типа host (A-запись). Чтобы создать статическую запись, необходимо выполнить:

Наименование	Описание
<b>Шаг 1.</b> Добавить запись	Нажать на кнопку <b>Добавить</b> , задать <b>Название</b> и <b>Описание</b> (опционально)
<b>Шаг 2.</b> Указать FQDN	Задать <b>Fully Qualified Domain Name (FQDN)</b> статической записи, например, <i>www.example.com</i>
<b>Шаг 3.</b> Указать IP-адреса	Задать список IP-адресов, которые сервер UserGate будет возвращать при запросе данного FQDN

## 5.6 Поддержка WCCP

Web Cache Communication Protocol (WCCP) – разработанный компанией [Cisco](#) протокол перенаправления контента. Предоставляет механизм перенаправления потоков трафика в реальном времени, имеет встроенные [масштабирование](#), [балансировку нагрузки](#), [отказоустойчивость](#). При использовании WCCP, WCCP-сервер принимает HTTP-запрос от клиентского браузера и перенаправляет его на один или несколько WCCP-клиентов. WCCP-клиент получает данные из интернет и возвращает их в браузер клиента. Доставка данных клиенту может происходить как через WCCP-сервер, так и минуя его, в соответствии с правилами маршрутизации.

UserGate может выступать в качестве WCCP-клиента. В качестве WCCP-сервера обычно выступает маршрутизатор. Для трафика, полученного через WCCP, можно применять все доступные механизмы фильтрации.

Сервисная группа WCCP - это набор серверов WCCP (роутеры, коммутаторы) и клиентов WCCP (UserGate) с общими настройками перенаправления трафика. Сервера, указанные в одной сервисной группе, должны иметь идентичные настройки.

Для настройки WCCP-клиента в UserGate необходимо выполнить следующие шаги:

Настройка сети

62 / 204

Наименование	Описание
<b>Шаг 1.</b> Настройте WCCP сервер	Произведите настройку сервера WCCP в соответствии с инструкцией на WCCP-сервер
<b>Шаг 2.</b> Настроить сервисные группы WCCP	В консоли UserGate в разделе <b>Сеть --&gt; WCCP</b> нажать на кнопку <b>Добавить</b> и создать одну или несколько сервисных групп WCCP.

При создании сервисной группы укажите следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или отключает данную сервисную группу.
<b>Название</b>	Имя сервисной группы.
<b>Описание</b>	Описание сервисной группы.
<b>Сервисная группа</b>	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу.
<b>Приоритет</b>	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP.
<b>Пароль</b>	Пароль, необходимый для аутентификации UserGate в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
<b>Способ перенаправления трафика</b>	<p>Определяет способ перенаправления трафика с серверов WCCP на UserGate. Возможны значения:</p> <ul style="list-style-type: none"> <li>gre - используя туннель Generic Routing Encapsulation (GRE).</li> <li>L2 - используя перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес UserGate.</li> </ul> <p>Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и UserGate должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.</p> <p>Важно! Для трафика, полученного через WCCP-туннель, в качестве IP источника UserGate будет использовать IP-адрес компьютера клиента, а зона источника не будет определена, поэтому в правилах фильтрации для зоны источника не следует явно указывать зону (оставить Any).</p>
<b>Способ возврата трафика</b>	<p>Определяет способ перенаправления трафика с UserGate на серверы WCCP. Возможны значения:</p> <ul style="list-style-type: none"> <li>gre - используя туннель Generic Routing Encapsulation (GRE).</li> <li>L2 - используя перенаправление L2. В этом случае UserGate (WCCP клиент) изменяет MAC-адрес назначения в пакете на адрес роутера (WCCP сервер).</li> </ul>

	Перенаправление L2 как правило требует меньше ресурсов, чем gre, но сервер WCCP и UserGate должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
<b>Порты для перенаправления</b>	<p>Порты для перенаправления. Укажите здесь порты назначения трафика. При необходимости указать несколько портов, укажите их через запятую, например:</p> <p>80, 442, 8080</p> <p>Если необходимо перенаправлять трафик на основании значений портов источника, то необходимо выделить чекбокс <b>Порт источника</b>.</p> <p>Важно! UserGate может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на UserGate с другими портами, будет отправляться в интернет без фильтрации.</p>
<b>Протокол</b>	Укажите протокол - TCP или UDP.
<b>Роутеры WCCP</b>	Укажите IP-адреса серверов WCCP (роутеры).
<b>Способ назначения</b>	<p>При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. Возможны варианты:</p> <ul style="list-style-type: none"> <li>• Хэш - распределение трафика на основе хэша, вычисляемому по указанным полям IP-пакета. Альтернативный хэш - если указан, то WCCP-сервер будет использовать его при превышении определенного количества пакетов, отправленных на WCCP-клиента с использованием обычного хэша. Поля IP-пакета, используемые для получения хэша, должны отличаться для вычисления основного и альтернативного хэшей.</li> <li>• Маска - распределение трафика на основе вычисления операции AND между маской и выбранным заголовком пакета. При выборе маски проконсультируйтесь с документацией производителя сервера WCCP.</li> </ul>

## 5.7 Маршруты

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей. Маршрут применяется локально к тому узлу кластера, на котором он создается.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Выбрать узел кластера	В случае наличия кластера выбрать в выпадающем меню узел, на котором будет создан маршрут
<b>Шаг 2.</b> Задать название и описание данного маршрута	Указать имя для данного маршрута. Опционально можно задать описание маршрута
<b>Шаг 3.</b> Указать адрес назначения	Задать подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или

	172 .16.20.5/32
<b>Шаг 4.</b> Указать шлюз	Задать IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UserGate
<b>Шаг 5.</b> Указать интерфейс	Выбрать интерфейс, на который будет добавлен маршрут
<b>Шаг 6.</b> Указать метрику	Задать метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько

## 5.8 Протоколы динамической маршрутизации

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. UserGate обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов.

Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно так же просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически.

### Примечание

Если в системе настроены статические шлюзы, то маршруты по умолчанию, полученные от протоколов динамической маршрутизации игнорируются.

UserGate поддерживает работу двух протоколов маршрутизации - OSPF и BGP.

### 5.8.1 OSPF

OSPF ([Open Shortest Path First](#)) - протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы (АС). Подробно о работе протокола OSPF читайте в соответствующей технической документации.

Для настройки OSPF в UserGate необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Включить OSPF-роутер	В консоли UserGate в разделе <b>Сеть --&gt; OSPF --&gt; OSPF-роутер</b> нажать на кнопку <b>Настройки</b> и настроить параметры OSPF-роутера
<b>Шаг 2.</b> Выбрать интерфейсы, через которые	В консоли UserGate в разделе <b>Сеть --&gt; OSPF --&gt; Интерфейсы</b> нажать

OSPF-роутер будет получать/распространять информацию от других маршрутизаторов	на кнопку <b>Добавить</b> и настроить параметры интерфейса. Добавить столько интерфейсов, сколько необходимо для работы OSPF в вашей организации
<b>Шаг 3.</b> Задать область OSPF (area)	<p>В консоли UserGate в разделе <b>Сеть --&gt; OSPF --&gt; Области</b> нажать на кнопку <b>Добавить</b> и настроить параметры области OSPF. Обязательно требуется указать созданные на предыдущем шаге интерфейсы, через которые область будет доступна другим маршрутизаторам.</p> <p>Добавить столько областей, сколько необходимо для работы OSPF в вашей организации</p>

При настройке OSPF-роутера необходимо указать следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или выключает использование данного OSPF-роутера
<b>Идентификатор роутера</b>	IP-адрес роутера. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам UserGate
<b>Redistribute</b>	Распространять другим OSPF-роутерам маршруты в непосредственно подключенные к UserGate сети (connected) или маршруты, добавленные администратором в разделе <b>Маршруты</b> (kernel)
<b>Метрика</b>	Установить метрику распространяемым маршрутам
<b>Default originate</b>	Оповещать другие роутеры о том, что данный роутер имеет маршрут по умолчанию

При настройке интерфейсов OSPF укажите следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или отключает использование данного интерфейса
<b>Интерфейс</b>	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF
<b>Стоимость</b>	Стоимость канала данного интерфейса. Данное значение передается в LSA (объявления о состоянии канала, link-state advertisement) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию 1
<b>Приоритет</b>	Целое число от 0 до 255. Чем больше значение, тем выше шанс у маршрутизатора стать назначенным маршрутизатором (designated router) в сети для рассылки LSA. Значение 0 делает назначение для данного маршрутизатора невозможным. Значение по умолчанию 1
<b>Интервал hello</b>	Время в секундах, через которое маршрутизатор посылает hello-пакеты. Это время должно быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию 10 секунд
<b>Интервал dead</b>	Интервал времени в секундах, по истечении которого соседний маршрутизатор считается неработающим. Время исчисляется от момента приема последнего пакета hello от соседнего

	маршрутизатора. Значение по умолчанию 40 секунд
<b>Интервал повторения</b>	Устанавливает временный интервал перед повторной отсылкой пакета LSA. Значение по умолчанию 5 секунд
<b>Задержка передачи</b>	Устанавливает примерное время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state). Значение по умолчанию 1 секунда
<b>Аутентификация Вкл</b>	Включает требование аутентификации каждого принимаемого роутером OSPF-сообщения. Аутентификация обычно используется для предотвращения инъекции фальшивого маршрута от нелегитимных маршрутизаторов
<b>Тип авторизации</b>	<p>Может быть:</p> <ul style="list-style-type: none"> <li>• <b>Plain</b> - передача ключа в открытом виде для аутентификации роутеров. Необходимо указать значение поля <b>Ключ</b></li> <li>• <b>Digest</b> - использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Необходимо указать <b>Ключ</b> и <b>MD5 key ID</b>. Эти параметры должны быть идентичными на всех роутерах для нормальной работы</li> </ul>

При настройке области OSPF укажите следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или отключает использование данной области
<b>Имя</b>	Имя для данной области
<b>Стоимость</b>	Стоимость LSA, анонсируемых в stub-области
<b>Идентификатор области</b>	Идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи <a href="#">IP-адреса</a> . Однако идентификаторы зон не являются IP-адресами и могут совпадать с любым назначенным IP-адресом
<b>Тип авторизации</b>	<p>Может быть:</p> <ul style="list-style-type: none"> <li>• <b>Нет</b> - не требовать авторизацию OSPF-пакетов</li> <li>• <b>Plain</b> - передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов</li> <li>• <b>Digest</b> - использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов</li> </ul> <p>Идентификация на уровне интерфейсов имеет приоритет над авторизацией на уровне зоны</p>
<b>Тип области</b>	<p>Определяет тип области. Поддерживаются следующие типы областей:</p> <ul style="list-style-type: none"> <li>• <b>Нормальная</b> - обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты</li> <li>• <b>Тупиковая (Stub)</b> - тупиковая зона, не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за</li> </ul>

	<p>границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR.</p> <ul style="list-style-type: none"> <li>• <b>NSSA</b> - Not-so-stubby. Зона NSSA определяет дополнительный тип LSA – LSA type 7. В NSSA зоне может находиться пограничный маршрутизатор (ASBR)</li> </ul>
<b>Не суммировать</b>	Запрещает инъекцию суммированных маршрутов в тупиковые типы областей
<b>Интерфейсы</b>	Выбор интерфейсов OSPF, на которых будет доступна данная зона
<b>Виртуальные ссылки</b>	<p>Специальное соединение, которое позволяет соединять, например, разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя ABR.</p> <p>Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение или как backup на случай выхода из строя основных соединений.</p> <p>Можно указать идентификаторы маршрутизаторов, которые доступны через данную зону</p>

### Примечание

При работе протокола OSPF в кластере отказоустойчивости в режиме Active-Passive, узел, который обладает ролью Slave, автоматически назначает стоимость для всех своих интерфейсов и для списков редистрибуции в 2 раза выше, чем установленная на узле стоимость. Тем самым обеспечивается приоритет Master-узла в маршрутизации трафика.

## 5.8.2 BGP

BGP ([Border Gateway Protocol](#)) - динамический протокол маршрутизации, относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP - External Gateway Protocol). На текущий момент является основным [протоколом](#) динамической [маршрутизации](#) в [интернете](#). Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протоколы внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети. Подробно о работе протокола BGP читайте в соответствующей технической документации.

Для настройки BGP в UserGate необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Включить BGP-роутер	В консоли UserGate в разделе <b>Сеть --&gt; BGP --&gt; BGP-роутер</b> нажать на кнопку <b>Настройки</b> и настроить параметры BGP-роутера

<b>Шаг 2.</b> Добавить хотя бы одного BGP-соседа (пира)	В консоли UserGate в разделе <b>Сеть --&gt; BGP --&gt; BGP-соседи</b> нажать на кнопку <b>Добавить</b> и настроить параметры маршрутизатора, относящегося к соседней АС. Добавить столько соседей, сколько необходимо
<b>Шаг 3.</b> Опционально. Задать фильтры и Routemap для ограничения количества получаемых маршрутов	В консоли UserGate в разделе <b>Сеть --&gt; BGP --&gt; Routemaps</b> или <b>Сеть --&gt; BGP --&gt; Фильтры</b> нажать на кнопку <b>Добавить</b> и настроить параметры Routemap/фильтров. Добавить столько Routemap/фильтров, сколько необходимо для работы BGP в вашей организации

При настройке BGP-роутера необходимо указать следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или отключает использование данного BGP-роутера.
<b>Идентификатор роутера</b>	IP-адрес роутера. Должен совпадать с одним из IP-адресов, назначенных сетевым интерфейсам UserGate.
<b>Номер автономной системы (АС)</b>	Автономная система - это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы задает принадлежность роутера к этой системе.
<b>Redistribute</b>	Позволяет распространять другим BGP-маршрутизаторам маршруты в непосредственно подключенные к UserGate-сети (connected), маршруты, добавленные администратором в разделе <b>Маршруты</b> (kernel) или маршруты, полученные по протоколу OSPF.
<b>Multiple path</b>	Включает балансировку трафика на маршруты с одинаковой стоимостью.
<b>Сети</b>	Список сетей, относящихся к данной АС.

Для добавления BGP-соседей нажмите кнопку **Добавить** и укажите следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или отключает использование данного соседа
<b>Интерфейс</b>	Один из существующих в системе интерфейсов, с которого должен быть доступен данный сосед
<b>Host</b>	IP-адрес соседа
<b>Описание</b>	Произвольное описание соседа
<b>Удаленная ASN</b>	Номер автономной системы, к которой относится сосед
<b>Вес</b>	Вес данных маршрутов, получаемых от данного соседа

<b>TTL</b>	Максимальное количество хопов, разрешенное до этого соседа
<b>Анонсировать себя в качестве следующего перехода (next-hop-self) для BGP</b>	Заменять значение next-hop-self на собственный IP-адрес, если сосед является BGP
<b>Multihop для eBGP</b>	Указывает, что до этого соседа не прямое соединение (более одного хопа)
<b>Route reflector client</b>	Указывает, является ли этот сосед клиентом Route reflector
<b>Soft reconfiguration</b>	Использовать soft reconfiguration (без разрыва соединений) для обновления конфигурации
<b>Default originate</b>	Анонсировать этому соседу маршрут по умолчанию
<b>Аутентификация</b>	Включает аутентификацию для данного соседа и задает пароль для аутентификации
<b>Фильтры BGP-соседей</b>	Ограничивает информацию о маршрутах, получаемых от соседей или анонсируемых к ним
<b>Routemaps</b>	Routemaps используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами

Routemap позволяет фильтровать маршруты при перераспределении и изменять различные атрибуты маршрутов. Для создания routemap необходимо указать следующие параметры:

Наименование	Описание
<b>Название</b>	Имя для данного routemap
<b>Действие</b>	Устанавливает действие для данного routemap, может принимать значения: <ul style="list-style-type: none"> <li>• <b>Разрешить</b> - разрешает прохождение данных, подпадающих под условия routemap</li> <li>• <b>Запретить</b> - запрещает прохождение данных, подпадающих под условия routemap</li> </ul>
<b>Сравнивать по</b>	Условия применения routemap, может принимать значения: <ul style="list-style-type: none"> <li>• <b>IP</b>. Если выбрано данное условие, то в закладке IP-адреса надо добавить все необходимые IP-адреса для данного условия</li> </ul> <p><b>AS путь</b>. Если выбрано данное условие, то в закладке AS-путь надо добавить все необходимые номера автономных сетей для данного условия. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания (<u> </u>), который интерпретируется как:</p> <ul style="list-style-type: none"> <li>• пробел</li> <li>• запятая</li> <li>• начало строки</li> </ul>

	<ul style="list-style-type: none"> <li>• конец строки</li> <li>• AS set delimiter { and }</li> <li>• AS confederation delimiter ( and )</li> </ul> <ul style="list-style-type: none"> <li>• <b>Community.</b> Если выбрано данное условие, то в закладке Community надо добавить строки всех необходимых BGP community для данного условия</li> </ul>
<b>Установить next hop</b>	Установить для отфильтрованных маршрутов значение next hop в указанный IP-адрес
<b>Установить вес</b>	Установить для отфильтрованных маршрутов вес в указанное значение
<b>Установить метрику</b>	Установить для отфильтрованных маршрутов метрику в указанное значение
<b>Установить предпочтение</b>	Установить для отфильтрованных маршрутов вес в указанное значение
<b>Установить AS-prepend</b>	Установить значение AS-prepend - список автономных систем, добавляемых для данного маршрута
<b>Community</b>	Установить значение для BGP community для отфильтрованных маршрутов

Фильтр позволяет фильтровать маршруты при перераспределении. При создании фильтров необходимо указать следующие параметры:

Наименование	Описание
<b>Название</b>	Имя для данного фильтра
<b>Действие</b>	Устанавливает действие для данного фильтра, может принимать значения: <ul style="list-style-type: none"> <li>• <b>Разрешить</b> - разрешает прохождение данных, попадающих под условия фильтра</li> <li>• <b>Запретить</b> - запрещает прохождение данных, попадающих под условия фильтра</li> </ul>
<b>Фильтровать по</b>	Условия применения фильтра, может принимать значения: <ul style="list-style-type: none"> <li>• <b>IP.</b> Если выбрано данное условие, то в закладке <b>IP-адреса</b> надо добавить все необходимые IP-адреса для данного условия</li> <li>• <b>AS путь.</b> Если выбрано данное условие, то в закладке <b>AS-путь</b> надо добавить все необходимые номера автономных сетей для данного условия</li> </ul>

## 6 ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Политики безопасности, правила межсетевого экрана, правила веб-безопасности и многие другие возможности UserGate могут быть применены к пользователям или группам пользователей. Возможность применения политик только к тем пользователям, которым это необходимо, позволяет администратору гибко настроить свою сеть в соответствии с потребностями организации.

Идентификация пользователя - это базисная функция UserGate. Пользователь считается идентифицированным, если система однозначно связала пользователя с IP-адресом устройства, с которого пользователь подключается к сети. UserGate использует различные механизмы для идентификации пользователей:

- Идентификация по явно указанному IP-адресу
- Идентификация по имени и паролю
- Идентификация пользователей терминальных серверов Microsoft с помощью специального агента терминального сервиса
- Идентификация пользователей с помощью агента авторизации (для Windows-систем)
- Идентификация с помощью протоколов NTLM, Kerberos

Идентификация пользователей по имени и паролю возможна через Captive-портал, который, в свою очередь, может быть настроен на идентификацию пользователей с помощью каталогов Active Directory, Radius, TACACS+, NTLM, Kerberos или локальной базы пользователей.

UserGate определяет следующие типы пользователей:

Наименование	Описание
Пользователь <b>Unknown</b>	Представляет множество пользователей, не идентифицированных системой
Пользователь <b>Known</b>	Представляет множество пользователей, идентифицированных системой. Методы идентификации пользователей могут быть различными и более подробно будут описаны далее в этой главе
Пользователь <b>Any</b>	Любой пользователь является объединением множеств пользователей <b>Known</b> и <b>Unknown</b>
Определенный пользователь	Конкретный пользователь, определенный и идентифицированный в системе, например, пользователь DOMAIN\User, идентифицированный с помощью авторизации в домене Active Directory

Пользователи и группы пользователей могут быть заведены на самом устройстве UserGate - это так называемые **локальные пользователи и группы** или могут быть получены с внешних каталогов, например, Microsoft Active Directory.

### 6.1 Группы

Группы пользователей позволяют объединить пользователей для более удобного управления политиками безопасности.

## 6.2 Пользователи

В данном разделе можно добавить локальных пользователей. Здесь же можно временно отключить пользователей или включить их заново.

Чтобы создать локального пользователя, необходимо указать единственный обязательный параметр - имя пользователя. Остальные параметры являются необязательными, но для корректной идентификации необходимо указать:

- Логин и пароль - для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
- IP-адрес или диапазон, MAC-адрес для идентификации с помощью комбинации MAC и IP-адресов. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанных MAC и/или IP-адреса.
- VLAN ID для идентификации пользователя по тегу VLAN. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанного VLAN.
- Почтовые адреса - email пользователя. Если указан, может быть использован для отсылки пользователю информации по электронной почте, например, 2-й фактор многофакторной организации.
- Номера телефонов - телефоны пользователя. Если указан, может быть использован для отсылки пользователю информации по SMS, например, 2-й фактор многофакторной организации.

В случае, если у пользователя указан и логин, и пароль, и IP/MAC/VLAN адреса, система использует идентификацию по адресу, то есть идентификация по адресу является более приоритетной.

Учетные записи пользователей LDAP здесь не отображаются, но эти пользователи также могут быть использованы в политиках безопасности.

## 6.3 Серверы авторизации

Серверы авторизации - это внешние источники учетных записей пользователей, например, LDAP-сервер, или серверы, производящие аутентификацию для UserGate, например, Radius, TACACS+, Kerberos, SAML. Система поддерживает следующие типы серверов авторизации:

- LDAP-коннектор
- Сервер авторизации пользователей Radius
- Сервер авторизации пользователей TACACS+
- Сервер авторизации Kerberos
- Сервер авторизации NTLM
- Сервер авторизации SAML (SSO)

Серверы авторизации Radius, TACACS+, NTLM, SAML могут осуществлять только авторизацию пользователей, в то время как LDAP-коннектор позволяет также получать информацию о пользователях и их свойствах.

В разделе **Серверы авторизации** находится кнопка **Сбросить авторизацию для всех пользователей**, которая стирает информацию в UserGate обо всех идентифицированных пользователях. После нажатия этой кнопки всем пользователям необходимо будет пройти авторизацию заново.

### 6.3.1 LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA. Пользователи и группы могут быть использованы при настройке правил фильтрации.
- Осуществлять авторизацию пользователей через домены Active Directory/FreeIPA с использованием методов авторизации Captive-портал, Kerberos, NTLM.

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

Наименование	Описание
<b>Вкл</b>	Включает или отключает использование данного сервера авторизации
<b>Название</b>	Название сервера авторизации
<b>SSL</b>	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу
<b>Доменное имя LDAP или IP-адрес</b>	IP-адрес контроллера домена или название домена LDAP. Если указано доменное имя, то UserGate получит адрес сервера LDAP с помощью DNS-запроса.
<b>Bind DN («login»)</b>	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или <a href="#">username@domain</a> . Данный пользователь уже должен быть заведен в домене
<b>Пароль</b>	Пароль пользователя для подключения к домену
<b>Домены LDAP</b>	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. Список доменов, указанный здесь будет использован для выбора на странице авторизации Captive-портала при включении соответствующей опции. Более подробно о настройке Captive-портала смотрите раздел <a href="#">Настройка Captive-портала</a> .
<b>Пути поиска</b>	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.
<b>Kerberos keytab</b>	Здесь можно загрузить keytab-файл для авторизации Kerberos. Подробно об авторизации Kerberos и создании keytab-файла смотрите в разделе <a href="#">Метод авторизации Kerberos</a> .  Важно! Рекомендуется загрузить keytab-файл даже в случае, если вы не планируете использовать авторизацию Kerberos. При загруженном keytab-файле UserGate использует механизм kerberos для получения списка пользователей и их групп с серверов LDAP, что очень сильно снижает нагрузку на серверы LDAP. Если у вас в организации серверы LDAP содержат большое количество объектов (более 1000 групп и пользователей) использование keytab-файла обязательно.

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.



## Примечание

Для авторизации пользователей с помощью LDAP-коннектора необходимо, чтобы пользователи входили в доменную группу Domain users.

Настройка LDAP-коннектора завершена. Для авторизации LDAP пользователей по имени и паролю необходимо создать правила Captive-портала. Более подробно о Captive-портале рассказывается в следующих главах руководства.

### 6.3.2 Сервер авторизации пользователей Radius

Сервер авторизации Radius позволяет авторизовать пользователей на серверах Radius, то есть UserGate выступает в роли Radius-клиента. При авторизации через Radius-сервер UserGate посылает на серверы Radius информацию с именем и паролем пользователя, а Radius-сервер отвечает, успешно прошла авторизация или нет.

Сервер Radius не может предоставить список пользователей в UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших авторизацию на сервере Radius) или **Unknown** (не прошедших авторизацию).

Для создания сервера авторизации Radius необходимо нажать на кнопку **Добавить**, выбрать **Добавить Radius-сервер** и указать следующие параметры:

Наименование	Описание
<b>Включен</b>	Включает или отключает использование данного сервера авторизации
<b>Название сервера</b>	Название сервера авторизации
<b>Секрет</b>	Общий ключ, используемый протоколом Radius для авторизации
<b>Хост</b>	IP-адрес сервера Radius
<b>Порт</b>	UDP-порт, на котором сервер Radius слушает запросы на авторизацию. По умолчанию это порт UDP 1812

После создания сервера авторизации необходимо настроить Captive-портал для использования метода авторизации Radius. Более подробно о Captive-портале рассказывается в следующих главах руководства.

### 6.3.3 Сервер авторизации пользователей TACACS+

Сервер авторизации TACACS+ позволяет авторизовать пользователей на серверах TACACS+. При авторизации через TACACS+ сервер UserGate посылает на серверы TACACS+ информацию с именем и паролем пользователя, а сервер TACACS+ отвечает, успешно прошла авторизация или нет.

Сервер TACACS+ не может предоставить список пользователей в UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших авторизацию на сервере TACACS+) или **Unknown** (не прошедших авторизацию).

Для создания сервера авторизации TACACS+ необходимо нажать на кнопку **Добавить**, выбрать **Добавить TACACS+-сервер** и указать следующие параметры:

Наименование	Описание
<b>Включен</b>	Включает или отключает использование данного сервера авторизации
<b>Название сервера</b>	Название сервера авторизации
<b>Секретный ключ</b>	Общий ключ, используемый протоколом TACACS+ для авторизации
<b>Адрес</b>	IP-адрес сервера TACACS+
<b>Порт</b>	UDP-порт, на котором сервер TACACS+ слушает запросы на авторизацию. По умолчанию это порт UDP 1812
<b>Использовать одно TCP-соединение</b>	Использовать одно TCP-соединение для работы с сервером TACACS+
<b>Таймаут (сек)</b>	Время ожидания сервера TACACS+ для получения авторизации. По умолчанию 4 секунды

### 6.3.4 Сервер авторизации пользователей SAML IDP

Сервер авторизации SAML IDP (Security Assertion Markup Language Identity Provider) позволяет авторизовать пользователей с помощью развернутой на предприятии системе Single Sign-On (SSO), например, Microsoft Active Directory Federation Service. Это позволяет пользователю единожды авторизовавшись в системе SSO прозрачно проходить авторизацию на всех ресурсах, поддерживающих авторизацию SAML. UserGate может быть настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для авторизации клиента.

Сервер SAML IDP не может предоставить свойства пользователей в UserGate и, если не настроено подключение к домену AD с помощью LDAP-коннектора, поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших авторизацию на сервере SAML) или **Unknown** (не прошедших авторизацию).

Для использования авторизации с помощью сервера SAML IDP необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать DNS-записи для сервера UserGate	На контроллере домена создать DNS-записи соответствующую серверу UserGate для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть <b>Trusted</b> .

<b>Шаг 2.</b> Настроить DNS-серверы на UserGate	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
<b>Шаг 3.</b> Изменить адрес Домен auth captive-портала	Изменить адрес <b>Домен auth captive-портала</b> в разделе <b>Настройки</b> на созданную на предыдущем шаге запись DNS. Подробно об изменении адреса домена Auth Captive-портала смотрите в разделе <a href="#">Общие настройки</a> .
<b>Шаг 4.</b> Настроить сервер SAML IDP	Добавить на сервере SAML IDP запись о сервис-провайдере USERGATE, указывая созданное на шаге 1 FQDN имя.
<b>Шаг 5.</b> Создать сервер авторизации пользователей SAML IDP	Создать в USERGATE сервер авторизации пользователей SAML IDP.

Для создания сервера авторизации пользователей SAML IDP необходимо в разделе **Пользователи и устройства --> Серверы авторизации** нажать на кнопку **Добавить**, выбрать **Добавить SAML IDP-сервер** и указать следующие параметры:

Наименование	Описание
<b>Включен</b>	Включает или отключает использование данного сервера авторизации
<b>Название сервера</b>	Название сервера авторизации
<b>Описание</b>	Описание сервера авторизации
<b>SAML metadata URL</b>	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии на кнопку <b>Загрузить</b> происходит заполнение необходимых полей настройки сервера авторизации данными, полученными из xml-файла. Это предпочтительный метод настройки сервера авторизации SAML IDP. Подробно о сервере SAML смотрите в соответствующей документации
<b>Сертификат SAML IDP</b>	Сертификат, который будет использован в SAML-клиенте. Возможны варианты: <ul style="list-style-type: none"> <li>Создать новый сертификат из скачанного - если при настройке был использован метод загрузки xml- файла, то сертификат автоматически создается и ему назначается роль SAML IDP (смотрите раздел <b>Сертификаты</b>)</li> <li>Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе <b>Сертификаты</b>, и ему не должна быть назначена роль. После создания и сохранения сервера авторизации этому сертификату будет назначена роль SAML IDP</li> <li>Не использовать сертификат</li> </ul>
<b>Single sign-on URL</b>	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации
<b>Single sign-on binding</b>	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты <b>POST</b> и <b>Redirect</b> . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной

	информации
<b>Single logout URL</b>	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации
<b>Single logout binding</b>	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты <b>POST</b> и <b>Redirect</b> . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации

### 6.3.5 Сервер авторизации NTLM

Авторизация NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации с помощью NTLM сервер UserGate работает с контроллерами домена, которые выполняют проверку пользователя, который получает доступ в интернет.

Сервер NTLM не может предоставить список пользователей в UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших авторизацию на сервере NTLM) или **Unknown** (не прошедших авторизацию).

Авторизация NTLM может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан. Настройка UserGate не отличается от режима работы авторизации.

Для настройки авторизации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Настроить синхронизацию времени с контроллером домена	В настройках UserGate включить синхронизацию времени с серверами NTP, в качестве основного и - опционально - запасного NTP-сервера указать IP-адреса контроллеров домена.
<b>Шаг 2.</b> Создать DNS-запись для сервера UserGate	На контроллере домена создать DNS-записи, соответствующие серверу UserGate для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc  В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть <b>Trusted</b> .
<b>Шаг 3.</b> Изменить адрес <b>Домен Auth Captive-портала</b>	Изменить адрес <b>домена Auth Captive-портала</b> и опционально адрес <b>домена Logout Captive-портала</b> в разделе <b>Настройки</b> .  Для домена <b>Auth Captive-портала</b> необходимо указать созданную на предыдущем шаге запись DNS.  Для домена <b>Logout Captive-портала</b> необходимо указать созданную на предыдущем шаге запись DNS.  Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе <a href="#">Общие настройки</a> .

<p><b>Шаг 4.</b> Добавить NTLM-сервер авторизации</p>	<p>В разделе <b>Серверы авторизации</b> нажать на кнопку <b>Добавить</b>, выбрать <b>Добавить NTLM-сервер</b> и указать название и имя домена Windows. Для корректной работы авторизации NTLM, необходимо, чтобы указанное здесь имя домена резолвилось в IP-адреса контроллеров домена.</p>
<p><b>Шаг 5.</b> Создать правило Captive-портала с авторизацией NTLM</p>	<p>Настроить Captive-портал для использования метода авторизации NTLM. Более подробно о Captive-портале рассказывается в следующих главах руководства.</p>
<p><b>Шаг 6.</b> Разрешить доступ к сервису HTTP(S) для зоны</p>	<p>В разделе <b>Зоны</b> разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM.</p>
<p><b>Шаг 7.</b> Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей</p>	<p>На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса UserGate в качестве адреса прокси сервера.</p> <p>Важно! Вместо IP-адреса можно использовать доменное имя, но для NTLM важно, чтобы это имя было не из домена Active Directory, иначе Windows-компьютер будет пытаться использовать авторизацию Kerberos.</p> <p>Важно! В настройках UserGate имена, используемые в качестве домена для auth.captive и logout.captive, не должны быть из домена Active Directory, иначе Windows-компьютер будет пытаться использовать авторизацию Kerberos.</p>
<p><b>Шаг 8.</b> Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон</p>	<p>На компьютерах пользователей зайдите в <b>Панель управления --&gt; Свойства браузера --&gt; Безопасность</b>, выберите зону <b>Интернет --&gt; Уровень безопасности --&gt; Другой --&gt; Проверка подлинности пользователя</b> и установите <b>Автоматический вход в сеть с текущим именем пользователя и паролем</b></p> <p>(Control panel --&gt; Internet options --&gt; Security, выберите зону <b>Internet --&gt; Custom level --&gt; User Authentication --&gt; Logon</b> и установите <b>Automatic logon with current name and password</b>)</p> <p>Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).</p>

### 6.3.6 Метод авторизации Kerberos

Авторизация Kerberos позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации через Kerberos сервер UserGate работает с контроллерами домена, которые выполняют проверку пользователя, который получает доступ в интернет.

Авторизация Kerberos может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан.

Для авторизации Kerberos необходимо выполнить следующие действия:

Наименование	Описание
--------------	----------

<p><b>Шаг 1.</b> Создать DNS-записи для сервера UserGate</p>	<p>На контроллере домена создать DNS-записи соответствующую серверу UserGate для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc</p> <p>В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть <b>Trusted</b>.</p> <p><b>Важно!</b> Для корректной работы создайте записи типа A, не используйте CNAME-записи.</p>
<p><b>Шаг 2.</b> Создать пользователя для сервера UserGate</p>	<p>Создать пользователя в домене AD, например, <a href="#">kerb@domain.loc</a> с опцией <b>password never expires</b>. Установите пароль пользователю kerb.</p> <p>Важно! Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя kerb или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя kerb.</p> <p>Важно! Не используйте в качестве пользователя для Kerberos пользователя, созданного для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.</p>
<p><b>Шаг 3.</b> Создать keytab файл</p>	<p>На контроллере домена, создать keytab файл, выполнив следующую команду <b>из-под администратора</b> (команда в одну строку!):</p> <pre>ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab</pre> <p>Введите пароль пользователя kerb.</p> <p>Важно! Команда чувствительна к регистру букв. В данном примере:</p> <p>auth.domain.loc - DNS-запись, созданная для сервера UserGate на шаге 1</p> <p>DOMAIN.LOC - Kerberos realm domain, обязательно большими буквами!</p> <p><a href="#">kerb@DOMAIN.LOC</a> - имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!</p>
<p><b>Шаг 4.</b> Настроить DNS-серверы на UserGate</p>	<p>В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена</p>
<p><b>Шаг 5.</b> Настроить синхронизацию времени с контроллером домена</p>	<p>В настройках UserGate включить синхронизацию времени с серверами NTP, в качестве основного и - опционально - запасного NTP-сервера указать IP-адреса контроллеров домена</p>
<p><b>Шаг 6.</b> Изменить адрес <b>Домен auth captive-портала</b></p>	<p>Изменить адрес <b>Домен auth captive-портала</b> и опционально адрес <b>Домен logout captive-портала</b> в разделе <b>Настройки</b> на созданные на предыдущем шаге записи DNS. Подробно об изменении адресов доменов смотрите в разделе <a href="#">Общие настройки</a>.</p>
<p><b>Шаг 7.</b> Создать LDAP-коннектор и загрузить в него keytab-файл</p>	<p>Создать сервер авторизации типа LDAP коннектор и загрузить полученный на предыдущем шаге keytab-файл.</p> <p>Важно! Не используйте в качестве пользователя для LDAP-коннектора,</p>

	<p>пользователя, созданного ранее для работы Kerberos. Необходимо использовать отдельную учетную запись.</p> <p>Подробнее о настройке LDAP-коннектора смотрите раздел <a href="#">LDAP-коннектор</a>.</p>
<b>Шаг 8.</b> Создать правило Captive-портала с авторизацией Kerberos	<p>Настроить Captive-портал для использования метода авторизации Kerberos. Более подробно о Captive-портале рассказывается в разделе <a href="#">Настройка Captive-портала</a>.</p>
<b>Шаг 9.</b> Разрешить доступ к сервису HTTP(S) для зоны	<p>В разделе <b>Зоны</b> разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью Kerberos</p>
<b>Шаг 10.</b> Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей	<p>На компьютерах пользователей указать обязательное использование прокси-сервера в виде FQDN-имени USERGATE, созданного на шаге 3</p>
<b>Шаг 11.</b> Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон	<p>На компьютерах пользователей зайдите в <b>Панель управления --&gt; Свойства браузера --&gt; Безопасность</b>, выберите зону <b>Интернет --&gt; Уровень безопасности --&gt; Другой --&gt; Проверка подлинности пользователя</b> и установите <b>Автоматический вход в сеть с текущим именем пользователя и паролем</b></p> <p><b>(Control panel --&gt; Internet options --&gt; Security, выберите зону Internet --&gt; Custom level --&gt; User Authentication --&gt; Logon и установите Automatic logon with current name and password)</b></p> <p>Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).</p>

### 6.3.7 Метод авторизации HTTP Basic

Авторизация Basic позволяет авторизовать пользователей с явно указанным прокси сервером по базе локальных и LDAP-пользователей. Не рекомендуется использовать данный тип авторизации поскольку имя пользователя и пароль передаются в открытом виде по сети. Авторизация HTTP Basic можно использовать для автоматической авторизации утилит командной строки, которым необходим доступ в интернет, например:

```
curl -x 192.168.179.10:8090 -U user:password http://www.msn.com
```

Для авторизации HTTP Basic необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать DNS-запись для сервера UserGate	<p>На контроллере домена создать DNS-записи, соответствующие серверу UserGate для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc</p> <p>В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть <b>Trusted</b>.</p>
<b>Шаг 2.</b> Изменить адрес <b>Домен</b>	<p>Изменить адрес <b>домена Auth Captive-портала</b> и опционально адрес <b>домена Logout</b></p>

<b>Auth Captive-портала</b>	<p><b>Captive-портала</b> в разделе <b>Настройки</b>.</p> <p>Для домена <b>Auth Captive-портала</b> необходимо указать созданную на предыдущем шаге запись DNS.</p> <p>Для домена <b>Logout Captive-портала</b> необходимо указать созданную на предыдущем шаге запись DNS.</p> <p>Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе <a href="#">Общие настройки</a>.</p>
<b>Шаг 3.</b> Создать правило Captive-портала с авторизацией HTTP Basic	<p>Настроить Captive-портал для использования метода авторизации HTTP Basic.</p> <p>При настройке, помимо метода <b>HTTP Basic</b>, необходимо добавить базу пользователей, по которой будет проверяться аутентификация (например, добавить методы аутентификации Локальный пользователь или Сервер LDAP).</p> <p>Более подробно о Captive-портале рассказывается в следующих главах руководства</p>
<b>Шаг 4.</b> Разрешить доступ к сервису HTTP(S) для зоны	<p>В разделе <b>Зоны</b> разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM</p>
<b>Шаг 5.</b> Настроить прокси-сервер на компьютерах пользователей	<p>На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса UserGate в качестве адреса прокси сервера.</p>

## 6.4 Профили авторизации

Профиль авторизации позволяет указать набор способов и параметров авторизации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах UserGate, например, Captive-портал, VPN, веб-портал и т.д. Чтобы создать профиль авторизации, необходимо в разделе **Пользователи и устройства - Профили авторизации** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
<b>Название</b>	Название Captive-профиля
<b>Описание</b>	Описание Captive-профиля
<b>Профиль MFA</b>	<p>Профиль мультифакторной авторизации. Должен быть предварительно создан в разделе <b>Профили MFA</b>, если планируется использовать мультифакторную авторизацию с данным профилем авторизации. Профиль определяет способ доставки одноразового пароля для второго метода авторизации. Более подробно о настройке профиля MFA смотрите в соответствующей главе далее.</p> <p>Важно! Мультифакторная авторизация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только те, где пользователь явно вводит свои учетные данные в веб-форму страницы авторизации. В связи с этим, мультифакторная авторизация невозможна для методов аутентификации Kerberos и NTLM</p>

<b>Время бездействия до отключения</b>	Данный параметр определяет, через сколько секунд UserGate переведет пользователя из <b>Known users</b> в <b>Unknown users</b> при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя).
<b>Время жизни авторизованного пользователя</b>	Данный параметр определяет, через сколько секунд UserGate переведет пользователя из <b>Known users</b> в <b>Unknown users</b> . По происшествии указанного времени пользователю потребуется повторно авторизоваться на Captive-портале
<b>Число неудачных попыток авторизации</b>	Разрешенное количество неудачных попыток авторизации через Captive-портал до блокировки учетной записи пользователя
<b>Время блокировки пользователя</b>	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации
<b>Методы аутентификации</b>	<p>Созданные ранее методы авторизации пользователей, например, сервер авторизации Active Directory или Radius. Если указано более одного метода авторизации, то они будут использоваться в порядке, в котором они перечислены в консоли.</p> <p>Также возможно использование встроенных механизмов авторизации, таких как:</p> <ul style="list-style-type: none"> <li>• Локальный пользователь - авторизация по базе данных локально заведенных пользователей.</li> <li>• Принять политику – не требуется авторизация, но прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный тип авторизации необходимо применять совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy.</li> <li>• HTTP Basic – авторизация с помощью устаревшего метода HTTP Basic.</li> </ul>

## 6.5 Настройка Captive-портала

Captive-портал позволяет авторизовать неизвестных пользователей (**Unknown users**) с помощью методов авторизации с использованием каталогов Active Directory, Radius, TACACS+, SAML IDP, Kerberos, NTLM или локальной базы пользователей. Кроме этого, с помощью Captive-портала можно настроить самостоятельную регистрацию пользователей с подтверждением идентификации через SMS или e-mail.

Следует помнить, что:

- Идентифицированные пользователи, например, у которых в свойствах пользователя явно указан IP-адрес, идентифицированные с помощью агентов авторизации терминальных серверов или для систем Windows, не авторизуются на Captive-портале. Такие пользователи уже относятся к типу **Known users** и не требуют дополнительной идентификации
- Авторизация с помощью Captive-портала возможна только для протоколов HTTP и HTTPS. Например, если вы создали правило межсетевого экрана, разрешающее доступ в интернет по протоколу FTP только для пользователя **Known users**, то пользователи не смогут получить доступ в интернет по этому протоколу до тех пор, пока они не станут идентифицированными, то есть не запустят у себя браузер и не пройдут авторизацию на Captive-портале
- Если Captive-портал использует метод авторизации Active Directory, то пользователь должен указывать в качестве логина свое доменное имя в формате DOMAIN\username или [username@domain](#)

Настройка Captive-портала сводится к следующим шагам:

Наименование	Описание
<b>Шаг 1.</b> Создать метод авторизации, например, авторизация с помощью домена Active Directory	В консоли UserGate в разделе <b>Пользователи и устройства --&gt; Серверы авторизации</b> нажать на кнопку <b>Добавить</b> и создать сервер авторизации
<b>Шаг 2.</b> Создать профиль авторизации, в котором указать необходимые методы авторизации	В консоли UserGate в разделе <b>Пользователи и устройства --&gt; Профили авторизации</b> нажать на кнопку <b>Добавить</b> и создать профиль авторизации, используя созданный ранее метод авторизации
<b>Шаг 3.</b> Создать Captive-профиль, в котором указать необходимые профили авторизации	В консоли UserGate в разделе <b>Пользователи и устройства --&gt; Captive-профили</b> нажать на кнопку <b>Добавить</b> и создать Captive-профиль, используя созданный ранее профиль авторизации
<b>Шаг 4.</b> Создать правило Captive-портала	Правило Captive-портала определяет трафик, к которому должны быть применены методы идентификации пользователей, указанные в Captive-профиле. В консоли UserGate в разделе <b>Пользователи и устройства --&gt; Captive-портал</b> нажать на кнопку <b>Добавить</b> и создать правило Captive-портала
<b>Шаг 5.</b> Настроить DNS для доменов auth.captive и logout.captive	Служебные доменные имена <b>auth.captive</b> и <b>logout.captive</b> используются UserGate для авторизации пользователей. Если клиенты используют в качестве DNS-сервера сервер UserGate, то ничего делать не надо. В противном случае необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса сервера UserGate, который подключен в клиентскую сеть. Альтернативное решение - настроить параметры <b>Домен auth captive-портала</b> и <b>Домен logout captive-портала</b> . Более детально эти параметры описаны в разделе <a href="#">Общие настройки</a> .

Создание методов авторизации подробно рассматривалось в предыдущих главах. Рассмотрим более подробно создание Captive-профиля и правил Captive-портала.

Чтобы создать Captive-профиль, необходимо в разделе **Captive-профили** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
<b>Название</b>	Название Captive-профиля
<b>Описание</b>	Описание Captive-профиля
<b>Шаблон страницы авторизации</b>	Выбрать шаблон страницы авторизации. Создавать страницы авторизации можно в разделе <b>Библиотеки --&gt; Шаблоны страниц</b> . Если необходимо настроить самостоятельную регистрацию пользователей с подтверждением по SMS или e-mail, то следует выбрать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth)
<b>Метод идентификации</b>	Метод, с помощью которого UserGate запомнит пользователя. Возможны 2 варианта: <ul style="list-style-type: none"> <li><b>Запоминать IP-адрес.</b> После успешной авторизации пользователя через</li> </ul>

	<p>Captive-портал UserGate запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относиться к данному пользователю. Данный метод позволяет идентифицировать данные, передаваемые по любому из протоколов семейства TCP/IP, но не будет корректно работать при наличии NAT-подключения между пользователями и сервером UserGate.</p> <p>Это рекомендуемое значение, устанавливаемое по умолчанию.</p> <ul style="list-style-type: none"> <li>• <b>Запоминать cookie.</b> После успешной авторизации пользователя через Captive-портал UserGate добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя. Данный метод позволяет авторизовать пользователей, находящихся за NAT-устройством, но авторизуется только протокол HTTP(S) и только в том браузере, в котором происходила авторизация через Captive-портал. Кроме этого, для авторизации HTTPS-сессий пользователя UserGate будет принудительно дешифровать все HTTPS-соединения. Для правил межсетевого экрана пользователь, идентифицированный по cookie, будет всегда определен как <b>Unknown user</b></li> </ul>
<b>Профиль авторизации</b>	Созданный ранее профиль авторизации, определяющий методы аутентификации
<b>URL для редиректа</b>	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL
<b>Разрешить браузерам запомнить авторизацию</b>	Включает возможность сохранить авторизацию в браузере на указанное время в часах. Для сохранения авторизационной информации используются cookie
<b>Предлагать выбор домена AD/LDAP на странице авторизации Captive-портала</b>	Если в качестве метода аутентификации используется авторизация с помощью Active Directory, то при включении данного параметра пользователь сможет выбрать имя домена из списка на странице авторизации. Если данный параметр не включен, пользователь должен явно указывать домен в виде DOMAIN\username или <a href="#">username@domain</a>
<b>Показывать CAPTCHA</b>	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей
<b>HTTPS для страницы авторизации</b>	Использовать HTTPS при отображении страницы авторизации Captive-портала для пользователей. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. Более подробно о сертификатах смотрите в разделе <a href="#">Управление сертификатами</a> .

Для настройки самостоятельной регистрации пользователей с подтверждением пароля с помощью SMS или e-mail необходимо настроить параметры на вкладке **Регистрация гостевых пользователей**. Следует помнить, что в этом случае необходимо использовать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).

Наименование	Описание
<b>Профиль</b>	Профиль оповещения, который будет использоваться для отсылки информации о созданном

<b>оповещения</b>	пользователе и его пароле. Может использоваться 2 типа - SMS и e-mail. Более подробно о создании профиля оповещения смотрите в главе <a href="#">Профили оповещений</a> .
<b>От</b>	Указать, от имени кого будут отправляться оповещения
<b>Тема оповещения</b>	Тема оповещения (только для e-mail-оповещений)
<b>Письмо оповещения</b>	Тело письма сообщения. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль.
<b>Дата и время окончания</b>	Время, когда учетная запись временного пользователя будет отключена
<b>Время жизни</b>	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена
<b>Длина пароля</b>	Определяет длину пароля для создаваемого пользователя
<b>Сложность пароля</b>	Определяет сложность пароля для создаваемого пользователя. Возможны варианты: Цифры Буквы цифры Буквы+цифры+спецсимволы
<b>Группы</b>	Группа для временных пользователей, в которую будут помещены создаваемые пользователи. О группах для временных пользователей читайте в главе <a href="#">Гостевой портал</a> .

Чтобы создать правило Captive-портала, необходимо нажать на кнопку **Добавить** в разделе **правил Captive-портала** и указать необходимые параметры:

Наименование	Описание
<b>Название</b>	Название правила Captive-портала.
<b>Описание</b>	Описание правила Captive-портала.
<b>Captive-профиль</b>	Выбрать Captive-профиль, созданный ранее. Доступно действие <b>Не использовать аутентификацию</b> , при выборе которого авторизация не будет требоваться.
<b>Записывать в журнал правил</b>	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
<b>Источник</b>	Адреса источника. В качестве источника можно указать определенную зону, например, зону LAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (Geo-IP).
<b>Назначение</b>	Адреса назначения. В качестве адресов можно указать определенную зону, например, зону WAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (Geo-IP).

<b>Категории</b>	Категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию.
<b>URL</b>	Списки URL, для которых будет применяться правило.
<b>Время</b>	Время, когда данное правило будет активно.

Таким образом, создав несколько правил Captive-портала, можно настроить различные политики идентификации пользователей для различных зон, адресов, категорий сайтов и времени.

### **Примечание**

Условия, указанные во вкладках правила, применяются согласно логике “И”, то есть требуют совпадения всех указанных условий для того, чтобы правило сработало. Если необходимо использовать логику “ИЛИ”, то это достигается путем создания нескольких правил.

### **Примечание**

Правила применяются в порядке, в котором они отображаются в консоли. Вы можете изменить порядок правил с помощью соответствующих кнопок.

### **Примечание**

При обработке правил применяется только первое сработавшее правило.

В случае, если необходимо сменить пользователя после его авторизации в системе или выйти из системы, необходимо перейти на URL <http://logout.captive> и нажать на кнопку **Выйти**.

## 6.6 Профили MFA (мультифакторной аутентификации)

Мультифакторная аутентификация - это метод идентификации пользователя, где используются два или более различных типа аутентификационных данных. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту учетной записи от несанкционированного доступа.

UserGate поддерживает мультифакторную аутентификацию с использованием имени пользователя и пароля в качестве первого типа аутентификации и следующих типов в качестве второго:

- TOTP (Time-based One Time Password) токена в качестве второго. TOTP-токен создает одноразовый пароль на основе времени, то есть время является параметром; более подробно о TOTP можно прочитать в [https://en.wikipedia.org/wiki/Time-based\\_One-time\\_Password\\_Algorithm](https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm). В качестве TOTP-токена могут

выступать различные устройства либо программное обеспечение, установленное на смартфоны пользователей, например, Google Authenticator

- SMS - получение одноразового пароля по SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в USERGATE или в доменной учетной записи в Active Directory
- Email - получение одноразового пароля по электронной почте. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в USERGATE или в доменной учетной записи в Active Directory.

Чтобы настроить мультифакторную аутентификацию, необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Настроить авторизацию с помощью Captive-портала	Мультифакторная авторизация работает только при авторизации пользователей с помощью Captive-портала. Смотрите раздел <a href="#">Настройка Captive-портала</a> для подробной информации.
<b>Шаг 2.</b> Создать профиль мультифакторной авторизации	В разделе консоли <b>Пользователи и устройства</b> --> <b>Профили MFA</b> создать профиль мультифакторной авторизации. При создании профиля указать необходимые настройки доставки второго фактора авторизации. Возможно создать 3 типа доставки: <ul style="list-style-type: none"> <li>• <b>MFA через TOTP</b> - доставка второго фактора авторизации с помощью токенов TOTP</li> <li>• <b>MFA через SMS</b> - доставка второго фактора авторизации с помощью SMS</li> <li>• <b>MFA через email</b> - доставка второго фактора авторизации с помощью email.</li> </ul>

Для способа доставки **MFA через TOTP** необходимо указать следующие параметры:

Наименование	Описание
<b>Название</b>	Название профиля MFA
<b>Описание</b>	Описание профиля MFA
<b>Инициализация TOTP</b>	Для получения токенов TOTP необходимо произвести первоначальную инициализацию устройства или ПО клиента. Для этого требуется ввести уникальный ключ в устройство или ПО клиента. Передать первоначальный код для инициализации TOTP можно следующими средствами: <ul style="list-style-type: none"> <li>• Показать на странице Captive-портала после первой успешной авторизации. Для этого варианта необходимо выбрать <b>Показать ключ на странице Captive -портала</b></li> <li>• Выслать с помощью SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в USERGATE или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки SMS (профиль SMPP)</li> <li>• Выслать с помощью email. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в USERGATE или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки email (профиль SMTP)</li> </ul>

<b>Показывать QR - код</b>	Показывать QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента
----------------------------	--

В случае, если пользователь утратил токен, администратор может потребовать повторной инициализации TOTP-токена. Для этого ему необходимо выбрать данного пользователя в списке пользователей (**Пользователи и устройства --> Пользователи**) и выбрать действие **Сбросить ключ TOTP**. При следующей авторизации пользователю будет предложено заново проинициализировать свой токен.

Для способа доставки **MFA через SMS** необходимо указать следующие параметры:

Наименование	Описание
<b>Название</b>	Название профиля MFA
<b>Описание</b>	Описание профиля MFA
<b>Профиль отправки MFA</b>	Профиль SMPP, который будет использован для отправки паролей с помощью сообщений SMS. Подробно о настройке профилей отсылки сообщений через SMS смотрите в разделе <a href="#">Профили оповещений</a> .
<b>От</b>	Указать, от имени кого будут отправляться оповещения
<b>Содержимое</b>	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.
<b>Время жизни MFA кода</b>	Срок действия одноразового пароля

Для способа доставки **MFA через email** необходимо указать следующие параметры:

Наименование	Описание
<b>Название</b>	Название профиля MFA
<b>Описание</b>	Описание профиля MFA
<b>Профиль отправки MFA</b>	Профиль SMTP, который будет использован для отправки паролей с помощью сообщений электронной почты. Подробно о настройке профилей отсылки сообщений по электронной почте смотрите в разделе <a href="#">Профили оповещений</a> .
<b>От</b>	Указать, от имени кого будут отправляться оповещения
<b>Тема</b>	Тема оповещения
<b>Содержимое</b>	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.

<b>Время жизни MFA кода</b>	Срок действия одноразового пароля
-----------------------------	-----------------------------------

## 6.7 Пользователи терминальных серверов

Терминальный сервер служит для удаленного обслуживания пользователя с предоставлением рабочего стола или консоли. Как правило, один терминальный сервер предоставляет свой сервис нескольким пользователям, а в некоторых случаях десяткам или даже сотням пользователей. Проблема идентификации пользователей терминального сервера состоит в том, что у всех пользователей сервера будет определен один и тот же IP-адрес, и UserGate не может корректно идентифицировать сетевые подключения пользователей. Для решения данной проблемы предлагается использование специального агента терминального сервиса.

Агент терминального сервиса должен быть установлен на все терминальные серверы, пользователей которых необходимо идентифицировать. Агент представляет собой сервис, который передает на сервер UserGate информацию о пользователях терминального сервера и об их сетевых соединениях. В силу специфики работы протокола TCP/IP, агент терминального сервиса может идентифицировать трафик пользователей, передаваемый только с помощью TCP и UDP протоколов. Протоколы, отличные от TCP/UDP, например, ICMP, не могут быть идентифицированы.

Для корректной идентификации пользователей требуется настроенный сервер Active Directory коннектор.

Чтобы начать работу с идентификацией пользователей на терминальных серверах, необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Разрешить сервис агент авторизации на необходимой зоне	В разделе <b>Сеть --&gt; Зоны</b> разрешить сервис <b>Агент авторизации</b> для той зоны, со стороны которой расположены серверы терминального доступа.
<b>Шаг 2.</b> Задать пароль агентов терминального сервера	В консоли UserGate в разделе <b>Пользователи и устройства --&gt; Терминальные серверы</b> нажать на кнопку <b>Настройки</b> и задать <b>Пароль агентов</b> терминального сервера
<b>Шаг 3.</b> Установить агент терминального сервера	Установить агент терминального сервера на все серверы, для которых необходимо идентифицировать пользователей. При установке следует задать IP-адрес сервера UserGate и заданный на предыдущем шаге пароль
<b>Шаг 4.</b> Включить необходимые серверы в консоли UserGate	После установки агентов в консоли UserGate появится список терминальных серверов. С помощью кнопок <b>Включить</b> и <b>Отключить</b> можно разрешить или запретить принимать идентификацию пользователей с выбранных серверов

UserGate теперь будет получать информацию о пользователях.

Если на терминальном сервере настроено несколько IP-адресов, то все они будут использованы для авторизации пользователей. Если необходимо ограничить выход пользователей в интернет только с

определенных IP-адресов терминального сервера, то необходимо внести изменения в конфигурационный файл агента авторизации для терминальных серверов и перезапустить его сервис.

Файл конфигурации: C:\ProgramData\Entensys\Terminal Server Agent\tsagent.cfg

Исключаемые IP-адреса необходимо указать в виде:

ExcludeIP=IP1;IP2

## 6.8 Агент авторизации для Windows

Для пользователей, работающих на операционной системе Windows, входящих в домен Active Directory, существует еще один способ идентификации - использовать специальный агент авторизации. Агент представляет собой сервис, который передает на сервер UserGate информацию о пользователе, его имя и IP-адрес, соответственно, UserGate будет однозначно определять все сетевые подключения данного пользователя, и идентификация другими методами не требуется. Чтобы начать работу с идентификацией пользователей с помощью агента авторизации, необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Разрешить сервис агент авторизации на необходимой зоне	В разделе <b>Сеть --&gt; Зоны</b> разрешить сервис <b>Агент авторизации</b> для той зоны, со стороны которой находятся пользователи
<b>Шаг 2.</b> Задать пароль агентов терминального сервера	В консоли UserGate в разделе <b>Пользователи и устройства --&gt; Терминальные серверы</b> нажать на кнопку <b>Настройки</b> и задать <b>Пароль агентов</b> терминального сервера.
<b>Шаг 3.</b> Установить агент авторизации	<p>Установить агент авторизации на все компьютеры, для которых необходимо идентифицировать пользователей.</p> <p>Агент авторизации поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. С помощью административного шаблона администратор может задать IP-адрес и порт сервера UserGate, и заданный на предыдущем шаге пароль. Более подробно о развертывании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft.</p> <p>Агент может быть установлен и без использования групповых политик. Для этого необходимо установить агент из инсталлятора и указать необходимые параметры для подключения к серверу UserGate в следующих ключах реестра:</p> <pre>[HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client] "ServerIP"="" "ServerPort"="1813" "SharedKey"=""</pre>

UserGate теперь будет получать информацию о пользователях. В политиках безопасности можно использовать имена пользователей, как они указаны в Active Directory, для этого необходим настроенный коннектор Active Directory. Если коннектор не настроен, то можно использовать пользователей **Known** и **Unknown**.

## 6.9 Прокси-агент для Windows

Для пользователей, работающих на операционной системе Windows, существует возможность предоставить доступ в интернет через явно указанный прокси-сервер программам, которые не поддерживают работу через прокси-сервер. Иногда также возникает необходимость предоставить таким программам доступ в интернет в случае, когда UserGate не является шлюзом в интернет по умолчанию для пользовательских компьютеров. Для подобных случаев можно использовать прокси-агент. Прокси-агент пересылает все TCP-запросы, идущие не на локальные адреса, на UserGate, который выступает для них прокси-сервером.

### Примечание

Прокси-агент не авторизует пользователя на UserGate, таким образом, если необходима авторизация, то потребуется настроить один из способов авторизации пользователей, например, установить агент авторизации для Windows.

Установить прокси-агент возможно вручную либо с использованием политик Active Directory.

Если устанавливаете не политикой, то для настройки агента необходимо создать текстовый файл `utmagent.cfg` в директории `in C:\Documents and Settings\All Users\Application Data\Entensys\UTMAgent\`. В файле конфигурации следует указать:

```
ServerName=10.255.1.1
```

```
ServerHttpPort=8090
```

```
LocalNetwork=192.168.1.0/24; 192.168.0.0/24; 192.168.30.0/24;
```

`ServerName` и `ServerHttpPort` - IP-адрес и порт прокси-сервера на UserGate, по умолчанию это порт 8090.

`LocalNetwork` - список сетей, которые не нужно направлять в прокси. Сеть интерфейсов машины не направляется в прокси по умолчанию.

Сервис прокси-агента слушает локальный порт 8080.

После создания или изменения файла конфигурации необходимо перезапустить сервис прокси-агента.

Если вы устанавливаете через GPO, прокси-агент поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. Более подробно о развертывании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft

Все необходимые параметры для корректной работы прокси-агента задаются при настройке групповой политики. При установке параметры вносятся в реестр пользовательского компьютера и имеют приоритет

перед файлом .cfg. При удалении агента политикой значения реестра не удаляются, сохраняясь в ветке реестра:

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Entensys\UTMAgent

## 6.10 Управление гостевыми пользователями

UserGate позволяет создавать списки гостевых пользователей. Данная возможность может быть полезна для гостиниц, публичных Wi-Fi, сетей интернет, где необходимо идентифицировать пользователей и предоставить им доступ на ограниченное время.

Гостевые пользователи могут быть созданы заранее администратором системы или пользователям может быть предоставлена возможность самостоятельной регистрации в системе с подтверждением через SMS или e-mail.

Для создания списка гостевых пользователей администратором необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать администратора гостевых пользователей (опционально)	<ul style="list-style-type: none"><li>В разделе <b>Администраторы</b> нажать кнопку <b>Добавить</b> и создать профиль администратора, разрешающий <b>Гостевой портал</b> для чтения и записи в закладке <b>Разрешения для веб-консоли</b>. Данный профиль дает доступ в консоль управления временными пользователями</li><li>Создать учетную запись администратора и назначить ей созданную роль</li></ul> <p>Более подробно о создании администраторов UserGate смотрите соответствующий раздел руководства</p>
<b>Шаг 2.</b> Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа гостевых пользователей	В консоли UserGate в разделе <b>Группы</b> нажать на кнопку <b>Добавить</b> и создать группу, отметив поле <b>Группа для гостевых пользователей</b> . Более подробно о создании групп пользователей смотрите соответствующий раздел руководства
<b>Шаг 3.</b> Подключиться к консоли управления Гостевого портала	В браузере перейти на адрес <a href="https://IP_UserGate:8001/ta">https://IP_UserGate:8001/ta</a> Для авторизации необходимо использовать логин и пароль администратора устройства или администратора гостевых пользователей, созданного на шаге 1
<b>Шаг 4.</b> Создать список пользователей	В консоли нажать на кнопку <b>Добавить</b> и заполнить поля: <ul style="list-style-type: none"><li>Количество пользователей</li><li>Комментарий</li><li><b>Дата и время окончания</b> - время, когда учетная запись гостевого пользователя будет отключена</li><li><b>Длина пароля</b> - определяет длину пароля для создаваемого пользователя</li><li><b>Сложность пароля</b> - определяет сложность пароля для создаваемого пользователя. Возможны варианты:</li><li>Цифры</li></ul>

- Буквы цифры
- Буквы+цифры+специальные символы
- **Время жизни** - продолжительность времени с момента первой авторизации гостевого пользователя, по истечении которого учетная запись будет отключена
- **Группа** - созданная на шаге 2 группа, в которую будут помещены создаваемые пользователи

Список созданных пользователей можно посмотреть в разделе **Пользователи** консоли управления временными пользователями.

Для самостоятельной регистрации пользователей в системе необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать профиль оповещения SMPP (для подтверждения через SMS) или SMTP (для подтверждения через e-mail)	В разделе <b>Библиотеки</b> --> <b>Профили оповещений</b> нажать кнопку <b>Добавить</b> и создать профиль оповещения SMPP или SMTP. Более подробно о создании профилей оповещения смотрите раздел руководства <a href="#">Профили оповещений</a> .
<b>Шаг 2.</b> Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа временных пользователей	В консоли UserGate в разделе <b>Группы</b> нажать на кнопку <b>Добавить</b> и создать группу, отметив поле <b>Группа для гостевых пользователей</b> . Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
<b>Шаг 3.</b> Создать профиль Captive-портала, в котором указать использование профиля оповещений, для отсылки информации о созданной учетной записи	В разделе <b>Пользователи и устройства</b> в подразделе <b>Captive-профили</b> создать профиль, указав в нем использование созданного ранее профиля оповещения. Указать в качестве страницы авторизации шаблон <b>Captive portal: email auth</b> или <b>Captive portal: SMS auth</b> , в зависимости от способа отправки оповещения. Настроить сообщение оповещения, группу, в которую будут помещены временные пользователи, времена действия учетной записи. Более подробно о создании профилей оповещения смотрите раздел руководства <a href="#">Профили оповещений</a> .
<b>Шаг 4.</b> Создать правило Captive-портала, которое будет использовать созданный на предыдущем шаге Captive-профиль	В разделе <b>Пользователи и устройства</b> --> <b>Captive-портал</b> создать правило, которое будет использовать созданный ранее Captive-профиль. Более подробно о создании правил Captive-портала смотрите раздел руководства <a href="#">Настройка Captive-портала</a> .

## 6.11 RADIUS accounting

UserGate может быть настроен на обновление IP-адресов пользователей с помощью серверов RADIUS, отсылающих информацию RADIUS accounting. Такая работа зачастую необходима при интеграции UserGate в сети провайдеров, где пользователи получают динамические IP-адреса. Для обновления IP-адреса у пользователей необходимо выполнить следующие шаги:

Наименование	Описание
<b>Завести пользователя в UserGate</b>	Завести необходимых локальных пользователей в UserGate. Смотрите раздел <b>Пользователи</b> .
<b>Разрешить сервис Агент авторизации на требуемой зоне</b>	В разделе <b>Сеть --&gt; Зоны</b> , выберите зону, на интерфейс которой планируется отсылать Radius-accounting. Разрешите сервис <b>Агент авторизации</b> . Более подробно о настройке зон смотрите в разделе <b>Настройка зон</b> .
<b>Настроить пароль агентов терминального сервиса</b>	В разделе <b>Терминальные серверы</b> , нажмите на кнопку <b>Настройки</b> и укажите пароль агента терминального сервиса. Данный пароль будет использоваться в качестве Radius secret при настройке сервера Radius.
<b>Настроить сервер Radius</b>	<p>Настроить на Radius сервере отсылку информации Radius-accounting на сервер UserGate, указав в качестве IP-адреса сервера IP-адрес UserGate, порт - UDP 1813. Указать Radius secret, совпадающий с паролем агента для терминального сервера, указанным на предыдущем шаге.</p> <p>Настройте сервер таким образом, чтобы имя пользователя передавалось в атрибуте Radius User-Name (type=1), а IP-адрес пользователя в атрибуте Radius Framed-IP-Address (type=8)</p> <p>Более подробно о настройке сервера Radius смотрите в руководстве на используемый вами сервер Radius.</p>

После выполнения данной настройки, UserGate будет изменять IP-адрес пользователя на присылаемый сервером Radius-accounting адрес. В зависимости от передаваемой информации UserGate будет вести себя следующим образом:

Наименование	Описание
<b>Radius сервер прислал имя пользователя, который не заведен на UserGate</b>	На Accounting-запрос будет ответ Accounting reject.
<b>Radius сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Start или Interim-Update</b>	<p>Указанному пользователю присвоится переданный IP-адрес. Если у пользователя уже был IP-адрес, отличный от переданного, то пользователю будет присвоено 2 и более IP-адресов.</p> <p>Если пользователю уже присвоен данный IP-адрес, то ничего не происходит.</p> <p>Если этот IP-адрес присвоен другому пользователю, то он будет удален у того пользователя и будет присвоен пользователю, указанному в запросе.</p>
<b>Radius сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Stop</b>	У указанного пользователя удалится переданный IP-адрес.

## 6.12 Политики BYOD

Многие компании поддерживают работу сотрудников с персональных устройств, принадлежащих самим сотрудникам. Это так называемые устройства BYOD (Bring Your Own Device). UserGate дает администратору возможность управлять BYOD устройствами, например, установив ограничения на типы разрешенных устройств, на количество устройств, с которых пользователь может получить доступ к сети одновременно, или указав конкретные устройства, с которых будет разрешен доступ в интернет.

### Примечание

Управление BYOD требует наличия корректно настроенной авторизации пользователей через Captive-портал. Пользовательские устройства, не авторизованные с помощью Captive-портала, не могут управляться с помощью политик BYOD. Более подробно о Captive-портале смотрите в главе .

Для управления устройствами BYOD необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать правило Captive-портала	Подробнее о создании правил Captive-портала смотрите раздел <a href="#">Настройка Captive-портала</a> .
<b>Шаг 2.</b> Создать политику BYOD	Создать одно или несколько правил политики BYOD.

### Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

### Примечание

Если не создано ни одного правила, то разрешены все типы устройств.

Чтобы создать правило политики BYOD, необходимо нажать на кнопку **Добавить** в разделе правил **Политики BYOD** и указать необходимые параметры:

Наименование	Описание
--------------	----------

<b>Название</b>	Название правила политики BYOD.
<b>Описание</b>	Описание правила политики BYOD.
<b>Действие</b>	<b>Разрешить</b> - разрешает подключение к сети устройств, удовлетворяющих условиям правила <b>Запретить</b> - запрещает подключение к сети устройств, удовлетворяющих условиям правила.
<b>Подтверждение администратора</b>	Только для разрешающих правил. Если данная опция включена, то после первой успешной авторизации пользователя через Captive-портал устройство пользователя помещается в список устройств BYOD, но доступ в сеть не предоставляется до подтверждения данного устройства администратором.
<b>Разрешено устройств всего</b>	Только для разрешающих правил. Максимальное количество устройств, с которых пользователь может получать доступ в сеть. Если в правиле используются типы пользователей <b>Known</b> , <b>Unknown</b> или <b>Any</b> , то данный параметр не применяется.
<b>Разрешено устройств одновременно</b>	Только для разрешающих правил. Максимальное количество устройств, с которых пользователь одновременно может получать доступ в сеть. Если в правиле используются типы пользователей <b>Known</b> , <b>Unknown</b> или <b>Any</b> , то данный параметр не применяется.
<b>Пользователи и группы</b>	Список пользователей и групп пользователей, для которых применяется данное правило политики BYOD.
<b>Тип устройства</b>	Тип устройств, для которых применяется данное правило политики BYOD.

Устройства, с которых пользователи подключаются в сеть, отображаются в разделе **Пользователи и устройства --> Устройства BYOD**. Администратор может запретить доступ пользователя с определенного устройства, выбрав устройство в списке и нажав на кнопку **Отключить**, или разрешить доступ, нажав на кнопку **Включить**. Здесь же можно подтвердить доступ пользователя с определенного устройства в случае, если политика BYOD требует подтверждение устройства администратором.

## 7 ПОЛИТИКИ СЕТИ

Раздел **Политики сети** содержит следующие подразделы:

- Межсетевой экран
- NAT и маршрутизация
- Балансировка нагрузки
- Пропускная способность

С помощью политик сети администратор может настроить необходимый доступ в интернет для своих пользователей, опубликовать внутренние ресурсы сети в интернете, управлять скоростью передачи данных для определенных сервисов и приложений.

### **Примечание**

Правила, созданные в данных разделах, применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила.

Для предоставления пользователям доступа в интернет необходимо:

Наименование	Описание
<b>Шаг 1.</b> Создать правило NAT (опционально)	Если необходимо NATирование трафика. Смотрите раздел <a href="#">Правила NAT</a> .
<b>Шаг 2.</b> Создать разрешительное правило межсетевого экрана	Смотрите раздел <a href="#">Межсетевой экран</a> .

Для публикации внутреннего ресурса в интернете необходимо:

Наименование	Описание
<b>Шаг 1.</b> Создать правило DNAT или правило reverse-прокси	Смотрите раздел <a href="#">Правила DNAT</a> и <a href="#">Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси</a> .

Чтобы указать для определенного сервиса или адреса выход в интернет через альтернативного провайдера, необходимо:

Наименование	Описание
<b>Шаг 1.</b> Создать правило Policy based routing	Смотрите раздел <a href="#">Policy-based routing</a> .

Для того чтобы запретить или разрешить определенный тип трафика, проходящий через UserGate, необходимо:

Наименование	Описание
<b>Шаг 1.</b> Создать правило межсетевого экрана	Смотрите раздел <a href="#">Межсетевой экран</a> .

Для того чтобы распределить трафик между несколькими внутренними серверами, необходимо:

Наименование	Описание
<b>Шаг 1.</b> Создать правило Балансировки нагрузки	Смотрите раздел <a href="#">Балансировка нагрузки</a> .

Для того чтобы ограничить скорость для определенного сервиса или приложения, необходимо:

Наименование	Описание
<b>Шаг 1.</b> Создать правило Пропускной способности	Смотрите раздел <a href="#">Пропускная способность</a> .

## 7.1 Межсетевой экран

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип транзитного сетевого трафика, проходящего через UserGate. В качестве условий правила могут выступать зоны и IP-адреса источника/назначения, пользователи и группы, сервисы и приложения.

События срабатывания правил межсетевого экрана отображаются в журнале трафика (**Журналы и отчёты -- > Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

### Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

### Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инvertировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

## Примечание

Если не создано ни одного правила, то любой транзитный трафик через UserGate запрещен.

Чтобы создать правило межсетевого экрана, необходимо нажать на кнопку **Добавить** в разделе **Политики сети --> Межсетевой экран** и указать необходимые параметры.

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило
<b>Название</b>	Название правила
<b>Описание</b>	Описание правила
<b>Действие</b>	<b>Запретить</b> - блокирует трафик <b>Разрешить</b> - разрешает трафик
<b>Сценарий</b>	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе <a href="#">Сценарии</a> .  Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает
<b>Журналирование</b>	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: <ul style="list-style-type: none"><li>• Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.</li><li>• Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.</li></ul>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика.
<b>Пользователи</b>	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа <b>Any, Unknown, Known</b> . Для применения правил к конкретным пользователям или к пользователям типа <b>Known</b> необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе <a href="#">Пользователи и устройства</a> .
<b>Назначение</b>	Зона назначения трафика и/или списки IP-адресов назначения трафика.
<b>Сервис</b>	Тип сервиса, например, HTTP или HTTPS.

<b>Приложение</b>	Список приложений, для которых применяется данное правило.
<b>Время</b>	Интервалы времени, когда правило активно.

## 7.2 NAT и маршрутизация

С помощью правил NAT и маршрутизации администратор может создавать правила NAT, DNAT и правила Policy based routing. UserGate поддерживает NAT/DNAT для сложных протоколов, которые могут использовать динамические порты для своей работы. Поддерживаются протоколы FTP, PPTP, SIP, H323.

События срабатывания правил NAT, DNAT, порт-форвардинга, Policy-based routing и Network mapping отображаются в журнале трафика (**Журналы и отчёты --> Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

### 7.2.1 Правила NAT

Как правило, для предоставления пользователям доступа в интернет необходимо создать хотя бы одно правило NAT из зоны **Trusted** в зону **Untrusted**.

#### Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

#### Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инvertировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Чтобы создать правило NAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети --> NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило
<b>Название</b>	Название правила

<b>Комментарий</b>	Описание правила
<b>Тип</b>	Выбрать <b>NAT</b>
<b>SNAT IP (внешний адрес)</b>	<p>Явно указывает IP-адрес, на который будет заменен адрес источника при наттировании пакетов. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, то система будет использовать произвольный адрес из списка доступных IP-адресов, назначенных интерфейсам зоны назначения. Допускается указание диапазона IP-адресов, например:</p> <p>192.168.10.10-192.168.10.20</p> <p>В этом случае UserGate будет использовать все указанные адреса при Source NAT.</p> <p>Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана.</p>
<b>Журналирование</b>	<p>Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты:</p> <ul style="list-style-type: none"> <li>• Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.</li> <li>• Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.</li> </ul>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика.
<b>Назначение</b>	Зона назначения трафика и/или списки IP-адресов назначения трафика.
<b>Сервис</b>	Тип сервиса, например, HTTP, HTTPS или другой.

### Примечание

Рекомендуется создавать общие правила NAT, например, правило NAT из локальной сети (обычно зона **Trusted**) в интернет (обычно зона **Untrusted**), а разграничение доступа по пользователям, сервисам, приложениям осуществлять с помощью правил межсетевого экрана.

## 7.2.2 Правила DNAT

Правила DNAT обычно используются для публикации внутренних ресурсов сети в интернет. Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси. Более подробно о публикации ресурсов с помощью правил reverse-прокси описано в главе [Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси](#). Для публикации серверов, работающих по протоколам, отличным от HTTP/HTTPS, необходимо использовать публикацию DNAT.

## Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Вверх/Вниз** для изменения порядка применения правил.

## Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Чтобы создать правило DNAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети --> NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Вкл/Выкл	Включает или отключает правило.
Название	Название правила.
Комментарий	Описание правила.
Тип	Выбрать <b>DNAT</b> .
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: <ul style="list-style-type: none"><li>• Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.</li><li>• Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.</li></ul>
Источник	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
Назначение	Один из внешних IP-адресов сервера UserGate, доступный из сети интернет, куда адресован трафик внешних клиентов.
Сервис	Тип сервиса, который необходимо опубликовать, например, HTTP. Если не указан сервис, то будут опубликованы все сервисы.

	Важно! Нельзя опубликовать сервисы, которые используют следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.
<b>Адрес назначения DNAT</b>	IP-адрес компьютера в локальной сети, который публикуется в интернет.
<b>Включить SNAT</b>	При включении данной опции UserGate будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.

### 7.2.3 Правила порт-форвардинга

Правила порт-форвардинга работают аналогично правилам DNAT за исключением того, что эти правила позволяют изменить номер порта, по которому публикуется внутренний сервис. Чтобы создать правило порт-форвардинга, необходимо нажать на кнопку **Добавить** в разделе **Политики сети --> NAT и маршрутизация** и указать необходимые параметры.

#### **Примечание**

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

#### **Примечание**

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Комментарий</b>	Описание правила.
<b>Тип</b>	Выбрать <b>Порт-форвардинг</b> .
<b>Журналирование</b>	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты:

	<ul style="list-style-type: none"> <li>• Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.</li> <li>• Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.</li> </ul>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Назначение</b>	Списки IP-адресов назначения трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Порт-форвардинг</b>	<p>Переопределения портов публикуемых сервисов:</p> <ul style="list-style-type: none"> <li>• <b>Оригинальный порт назначения</b> - номер TCP/UDP-порта, на который пользователи шлют запросы.</li> <li>• Важно! Нельзя использовать следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.</li> <li>• <b>Новый порт назначения</b> - номер TCP/UDP-порта, на который будут пересылаться запросы пользователей на внутренний публикуемый сервер</li> </ul>
<b>Адрес назначения DNAT</b>	IP-адрес компьютера в локальной сети, который публикуется в интернете.
<b>Включить SNAT</b>	При включении данной опции UserGate будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.

## 7.2.4 Policy-based routing

Правила policy based routing обычно используются для указания определенного маршрута в интернет для определенных хостов и/или сервисов. Например, в организации используются 2 провайдера и необходимо весь HTTP-трафик пересылать через провайдера 1, а весь остальной - через провайдера 2. Для этого необходимо указать в качестве шлюза по умолчанию в интернет-шлюз провайдера 2 и настроить правило policy-based routing для HTTPS-трафика через шлюз провайдера 1.



### Примечание

Правила PBR не заменяют и не влияют на работу правил NAT. Для трансляции адресов, после правила PBR необходимо поставить соответствующее правило NAT.

## Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

## Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Чтобы создать правило policy-based routing, необходимо нажать на кнопку **Добавить** в разделе **Политики сети-->NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Комментарий</b>	Описание правила.
<b>Тип</b>	Выбрать <b>Policy-based routing</b> .
<b>Шлюз</b>	Выбор одного из существующих шлюзов. Вы можете добавить шлюз в разделе <b>Сеть --&gt; Шлюзы</b> .
<b>Журналирование</b>	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: <ul style="list-style-type: none"><li>• Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.</li><li>• Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.</li></ul>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Кроме IP-адреса можно указать список MAC-адресов, для которых будет применяться правило.
<b>Назначение</b>	Зона назначения трафика и/или списки IP-адресов назначения трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .

<b>Сервис</b>	Тип сервиса, например, HTTP, HTTPS или другой.
---------------	--

## 7.2.5 Network mapping

Правила Network mapping позволяют подменить адрес сети источника или назначения. Как правило это необходимо, если имеется несколько сетей с одинаковой адресацией, например, 192.168.1.0/24, и их необходимо объединить в единую маршрутизируемую сеть. Без подмены адресов сетей такое объединение совершить невозможно. Network mapping изменяет только адрес сети, оставляя адрес хоста без изменений, например, при замене сети источника с 192.168.1.0/24 на 192.168.2.0/24 хост 192.168.1.1 будет изменен на 192.168.2.1.

### Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

Чтобы создать правило **Network mapping**, необходимо нажать на кнопку **Добавить** в разделе **Политики сети --> NAT и маршрутизация** и указать необходимые параметры:

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Комментарий</b>	Описание правила.
<b>Тип</b>	Выбрать <b>Network mapping</b> .
<b>Журналирование</b>	<p>Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты:</p> <ul style="list-style-type: none"> <li>Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.</li> <li>Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.</li> </ul>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика.
<b>Назначение</b>	Списки IP-адресов назначения трафика.
<b>Сервис</b>	Тип сервиса, например, HTTP, HTTPS или другой.

<b>Network mapping</b>	<p>Задаются параметры подмены сетей.</p> <p><b>Направление:</b></p> <ul style="list-style-type: none"> <li>• Входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле <b>Новая IP-сеть/маска</b>.</li> <li>• Исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле <b>Новая IP-сеть/маска</b>.</li> <li>• <b>Новая IP-сеть/маска</b> - адрес сети, на которую будет производиться замена.</li> </ul>
------------------------	--

## 7.3 Балансировка нагрузки

UserGate позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена:

- Для внутренних серверов, публикуемых в интернете (DNAT).
- Для внутренних серверов без публикации.
- Для балансировки трафика, пересылаемого на внешние серверы (ферму) ICAP-серверов.
- Для балансировки трафика на серверы, публикуемые через reverse-прокси.

Балансировщик распределяет запросы, поступающие на IP-адрес виртуального сервера, на IP-адреса реальных серверов, используя при этом различные методы балансировки. Чтобы настроить балансировку, необходимо в разделе **Политики сети --> Балансировка нагрузки** создать правила балансировки.

Для создания правила балансировки для серверов TCP/IP необходимо выбрать пункт **Добавить балансировщик TCP/IP** и указать следующие параметры:

Наименование	Описание
<b>Включен</b>	Включает или отключает данное правило.
<b>Название</b>	Название правила балансировки.
<b>Описание</b>	Описание правила балансировки.
<b>IP-адрес виртуального сервера</b>	Необходимо выбрать из списка IP-адресов, назначенных на сетевые интерфейсы. При необходимости администратор может добавить дополнительные IP-адреса на желаемый интерфейс.
<b>Порт</b>	Порт, для которого необходимо производить балансировку нагрузки.
<b>Протокол</b>	Протокол - TCP или UDP - для которого необходимо производить балансировку нагрузки.
<b>Метод балансировки</b>	<p>Возможны 4 различных метода распределения нагрузки на реальные серверы:</p> <ul style="list-style-type: none"> <li>• <b>Round robin</b> - каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы .</li> <li>• <b>Weighted round robin</b> - работает аналогично Round robin, но загрузка реальных</li> </ul>

	<p>серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера.</p> <ul style="list-style-type: none"> <li>• <b>Least connections</b> - новое подключение передается на сервер, на который в данный момент установлено наименьшее число соединений.</li> <li>• <b>Weighted least connections</b> - работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера.</li> </ul>
<p><b>Реальные серверы</b></p>	<p>Добавляется пул реальных серверов, на которые перенаправляется трафик. Для каждого из серверов необходимо указать:</p> <ul style="list-style-type: none"> <li>• IP-адрес сервера.</li> <li>• <b>Порт сервера.</b> Порт, на который пересылать запросы пользователей.</li> <li>• <b>Вес.</b> Данный коэффициент используется для неравномерного распределения нагрузки на реальные серверы для режимов балансировки <b>weighted round robin</b> и <b>weighted least connections</b>. Чем больше вес, тем больше будет нагрузка на сервер.</li> <li>• <b>Режим.</b> Может быть два варианта:</li> <li>• <b>Шлюз</b> - для перенаправления трафика на виртуальный сервер используется маршрутизация.</li> <li>• <b>Маскарадинг</b> - для перенаправления трафика на виртуальный сервер используется DNAT</li> <li>• <b>Маскарадинг с подменой IP-источника (SNAT)</b> - аналогично маскарадингу, но при этом UserGate подменяет IP-адрес источника на свой.</li> </ul>
<p><b>Аварийный режим</b></p>	<p>Аварийный режим используется, когда не доступен ни один из реальных серверов. Для активации аварийного режима необходимо включить его и указать:</p> <ul style="list-style-type: none"> <li>• IP-адрес сервера.</li> <li>• <b>Порт сервера.</b> Порт, на который пересылать запросы пользователей.</li> <li>• <b>Режим.</b> Может быть два варианта:</li> <li>• <b>Шлюз</b> - для перенаправления трафика на виртуальный сервер используется маршрутизация.</li> <li>• <b>Максарадинг</b> - для перенаправления трафика на виртуальный сервер используется DNAT.</li> <li>• <b>Маскарадинг с подменой IP-источника (SNAT)</b> - аналогично маскарадингу, но при этом UserGate подменяет IP-адрес источника на свой.</li> </ul>
<p><b>Мониторинг</b></p>	<p>С помощью мониторинга можно настроить проверку реальных серверов на определение их работоспособности. Если проверка прошла неуспешно для реального сервера, он исключается из балансировки.</p>
<p><b>Режим</b></p>	<p>Способ мониторинга реальных серверов. Возможны варианты:</p> <ul style="list-style-type: none"> <li>• <b>ping</b> - проверить доступность узла с помощью утилиты ping.</li> <li>• <b>connect</b> - проверить работоспособность узла, установив TCP-соединение на определенный порт.</li> <li>• <b>negotiate</b> - проверить работоспособность узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. Для настройки этого режима следует выбрать тип сервиса (HTTP или DNS), строки <b>Запрос</b> и <b>Ожидаемый ответ</b>. Например, для HTTP-запроса: <p>Запрос: /robots.txt</p> </li></ul>

	<p>Ожидаемый ответ: Disallow: /bin/</p> <p>Строка запроса тут указывает на путь на реальных серверах, который будет использован в HTTP-запросе. Строка ожидаемого ответа содержит фрагмент возвращаемой веб-страницы.</p>
<b>Интервал проверки</b>	Интервал времени, через которое должна выполняться проверка.
<b>Время ожидания</b>	Интервал времени ожидания ответа на проверку .
<b>Число неудачных попыток</b>	Количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки.

### **Примечание**

Правила балансировки имеют более высокий приоритет и применяются до правил NAT/DNAT/Маршрутизации.

Балансировщик серверов ICAP позволяет распределить нагрузку на внешние серверы или ферму серверов ICAP, например, на внешнюю ферму серверов с антивирусным ПО. Данный балансировщик затем может быть использован в правилах ICAP. Для создания балансировщика серверов ICAP необходимо выбрать пункт **Добавить балансировщик ICAP** и указать следующие параметры:

Наименование	Описание
<b>Включен</b>	Включает или отключает данное правило.
<b>Название</b>	Название правила балансировки.
<b>Описание</b>	Описание правила балансировки.
<b>ICAP-профили</b>	Выбрать ICAP-профили серверов, на которые будет распределяться нагрузка. Более подробно о работе с серверами ICAP читайте в разделе <a href="#">Работа с внешними ICAP-серверами</a> .

Балансировщик серверов reverse-прокси позволяет распределить нагрузку на внутренние серверы или ферму серверов, публикуемую с помощью правил reverse-прокси. Данный балансировщик затем может быть использован в правилах reverse-прокси. Для создания балансировщика reverse-прокси необходимо выбрать пункт **Добавить балансировщик reverse-прокси** и указать следующие параметры:

Наименование	Описание
<b>Включен</b>	Включает или отключает данное правило.
<b>Название</b>	Название правила балансировки.

<b>Описание</b>	Описание правила балансировки.
<b>Reverse-прокси профили</b>	Выбрать reverse-прокси профили серверов, на которые будет распределяться нагрузка). Более подробно о публикации с помощью reverse-прокси читайте в разделе <a href="#">Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси</a> .

## 7.4 Пропускная способность

Правила управления пропускной способностью используются для ограничения канала для определенных пользователей, хостов, сервисов, приложений.

### Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

### Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Чтобы создать правило пропускной способности, необходимо нажать на кнопку **Добавить** в разделе **Политики сети --> Пропускная способность** и указать необходимые параметры.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Полоса пропускания</b>	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритетизации трафика DSCP. Создать дополнительные полосы пропускания можно в разделе <a href="#">Полосы пропускания</a> .
<b>Сценарий</b>	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе <b>Политики безопасности --&gt; Сценарии</b> .

	Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Пользователи</b>	Пользователи или группы пользователей, к которым применится правило.
<b>Назначение</b>	Зона назначения трафика и/или списки IP-адресов назначения трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Сервис</b>	Тип сервиса, например, HTTP, HTTPS или другой.
<b>Приложения</b>	Список приложений, для которых необходимо ограничить полосу пропускания.
<b>Время</b>	Время, когда данное правило активно.

## 8 ПОЛИТИКИ БЕЗОПАСНОСТИ

Раздел **Политики безопасности** содержит следующие подразделы:

- Фильтрация контента.
- Веб-безопасность.
- Инспектирование SSL.
- Система обнаружения вторжений (COB).
- Правила АСУ ТП.
- Сценарии.
- Защита почтового трафика.
- ICAP-серверы, ICAP-правила.
- Правила защиты DOS, профили DOS.

С помощью политик безопасности администратор может:

- Настроить фильтрацию HTTP-контента, например, запретить некоторым пользователям доступ к определенным категориям сайтов в заданное время или настроить антивирусную проверку веб-контента.
- Настроить опции веб-безопасности, например, включить принудительный безопасный поиск и блокировку рекламы.
- Настроить правила инспектирования SSL, например, для всех пользователей расшифровывать HTTPS для категории “Форумы” и для определенной группы - “Социальные сети”. После того как HTTPS расшифрован, к нему могут быть применены политики фильтрации контента и веб-безопасности.
- Включить и настроить параметры COB.
- Настроить проверку почтовых протоколов SMTP и POP3 на проверку на наличие спама и вирусов.
- Настроить журналирование или блокировку определенных команд АСУ ТП.
- Настроить выборочную передачу трафика на анализ на внешние серверы ICAP, например, на DLP-системы.
- Настроить публикацию HTTP/HTTPS серверов.

События срабатывания данных правил регистрируются в соответствующих журналах статистики.

Правила фильтрации контента, веб-безопасности и инспектирования SSL доступны в журнале веб-доступа (**Журналы и отчёты --> Журнал веб-доступа**).

Правила система обнаружения и предотвращения вторжений - в журнале COB (**Журналы и отчёты --> Журнал COB**).

Правила АСУ ТП - в журнале АСУ ТП (**Журналы и отчёты --> Журнал АСУ ТП**).

Правила Защита от DoS атак - в журнале трафика (**Журналы и отчёты --> Журнал трафика**).

Все правила журналируются только при включении опции **Журналирование** в параметрах правил.

### 8.1 Фильтрация контента

С помощью правил фильтрации контента администратор может разрешить или запретить определенный контент, передаваемый по протоколам HTTP и HTTPS, если настроено инспектирование HTTPS. Более того, UserGate может блокировать HTTPS-трафик без дешифрования контента, но только в случае применения правил блокирования по категориям контентной фильтрации UserGate URL filtering или по спискам URL, в которых указаны только имена хостов. В этих случаях UserGate использует SNI (Server Name Indication), а

при отсутствии SNI - значения хоста из SSL-сертификата из пользовательских запросов для определения домена.

В качестве условий правила могут выступать:

- Пользователи и группы.
- Наличие на веб-страницах определенных слов и выражений (морфология).
- Принадлежность сайтов категориям.
- URL.
- Зона и IP-адрес источника.
- Зона и IP-адрес назначения.
- Тип контента.
- Информация о реферере.
- Время.
- Useragent браузера пользователя.
- HTTP-метод.

---

### **Примечание**

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

---

---

### **Примечание**

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

---

---

### **Примечание**

Если не создано ни одного правила, то передача любого контента разрешена.

---

Чтобы создать правило контентной фильтрации, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности --> Фильтрация контента** и указать необходимые параметры.

Наименование	Описание
Вкл/Выкл	Включает или отключает правило.

---

<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Действие</b>	<p><b>Запретить</b> - блокирует веб-страницу.</p> <p><b>Предупредить</b> - предупреждает пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал.</p> <p><b>Разрешить</b> - разрешает посещение.</p>
<b>Записывать в журнал правил</b>	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.
<b>Проверять потоковым антивирусом UserGate</b>	Доступно только для правил с действием <b>Запретить</b> , т.е. при наличии вируса на странице ресурс будет запрещен. Если в правиле присутствуют другие условия (категории, время, и т.д.), то антивирусная проверка будет выполняться только при совпадении всех условий правила.
<b>Сценарий</b>	<p>Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе <a href="#">Сценарии</a>.</p> <p>Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.</p>
<b>Страница блокировки</b>	Указывает страницу блокировки, которая будет показана пользователю при блокировке доступа к ресурсу. Можно использовать внешнюю страницу, указав <b>Использовать внешний URL</b> , либо указать страницу блокировки UserGate. В этом случае можно выбрать желаемый шаблон страницы блокировки, который можно создать в разделе <a href="#">Шаблоны страниц</a> .
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Назначение</b>	Зона назначения трафика и/или списки IP-адресов назначения трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Пользователи</b>	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа <b>Any, Unknown, Known</b> . Для применения правил к конкретным пользователям или к пользователям типа <b>Known</b> необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе <a href="#">Пользователи и устройства</a> .
<b>Категории</b>	<p>Списки категорий UserGate URL filtering 4.0. Использование категорий требует наличия специальной лицензии. UserGate URL filtering 4.0 - это крупнейшая база электронных ресурсов, разделенных для удобства оперирования на 72 категории. В руках администратора находится управление доступом к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети и многие другие.</p> <p>Важно! Начиная с версии UserGate 5.0.6R6 администратор может переопределить категорию на любой сайт, на который по его мнению категория назначена не верно или не назначена совсем. Более подробно процедура изменения категории сайта описана в разделе <a href="#">Запросы в</a></p>

	<p><a href="#">белый список</a>.</p> <p>Важно! Блокировка по категориям сайтов может быть применена к трафику HTTPS без его дешифрования, но без показа страницы блокировки.</p>
<b>URL</b>	<p>Списки URL. При наличии соответствующей лицензии доступны для использования списки URL, обновляемые разработчиками UserGate, такие, как «Черный список UserGate», «Белый список UserGate», «Черный список Роскомнадзора», «Черный список фишинговых сайтов», «Поисковые системы без безопасного поиска». Администраторы также могут создавать собственные списки URL. Более подробно о работе со списками URL читайте в главе <a href="#">Списки URL</a>.</p> <p>Важно! Блокировка по спискам URL может быть применена к трафику HTTPS без его дешифрования, если в списках указаны только имена хостов (доменов), но без показа страницы блокировки.</p>
<b>Типы контента</b>	<p>Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе <a href="#">Типы контента</a>.</p>
<b>Морфология</b>	<p>Список баз словарей морфологии, по которым будут проверяться веб-страницы. При наличии соответствующей лицензии для использования доступны словари, обновляемые компанией UserGate, в том числе список материалов, запрещенных Министерством Юстиции Российской Федерации, словари по темам «Суицид», «Терроризм», «Порнография», «Нецензурные выражения», «Азартные игры», «Наркотики», «Защита детей ФЗ-436». Словари доступны на русском, английском, немецком, японском и арабском языках.</p> <p>Администраторы также могут создавать собственные словари. Более подробно о работе с морфологическими словарями читайте в главе <a href="#">Морфология</a>.</p>
<b>Время</b>	<p>Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе <a href="#">Календари</a>.</p>
<b>Useragent</b>	<p>Useragent пользовательских браузеров, для которых будет применено данное правило. Администратор может добавить необходимые ему Useragent в разделе <a href="#">Useragent браузеров</a>.</p>
<b>HTTP метод</b>	<p>Метод, используемый в HTTP-запросах, как правило, это POST или GET</p>
<b>Рефереры</b>	<p>Список URL, в котором указаны рефереры для текущей страницы, таким образом правило сработает, если для данной страницы реферер совпадет со списком указанных URL. Данный функционал удобно использовать, чтобы, например, разрешить доступ к сетям CDN (Content Delivery Network) только посещая определенные сайты, но запретить открытие контента CDN напрямую.</p>

## 8.2 Веб-безопасность

С помощью раздела **Веб-безопасность** администратор может включить дополнительные параметры веб-безопасности для протоколов HTTP и HTTPS, если настроено инспектирование HTTPS. Доступны следующие параметры:

- Блокировка рекламы. Посещение безопасного сайта может быть связано с принудительным просмотром изображений нежелательного характера, размещенных, например, сбоку на странице. UserGate решает эту проблему, выступая в качестве «баннерорезки».
- Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователем. Инжектируемый скрипт будет вставлен в веб-страницы перед тегом </head>.
- Принудительное включение безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. С помощью данного инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту.
- Включение журналирования поисковых запросов пользователей.
- Блокировка приложений социальных сетей. Социальные сети играют большую роль в нашей повседневной жизни, но многие из них предоставляют игровые приложения, использование которых не приветствуется большинством компаний. UserGate может блокировать приложения, не затрагивая при этом обычную функциональность социальных сетей.

В качестве условий правила могут выступать:

- Источник трафика.
- Пользователи и группы.
- Время.

---

### Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

---

### Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

---

### Примечание

Если не создано ни одного правила, то дополнительные функции веб-безопасности не применяются.

---

Чтобы создать правило контентной фильтрации необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности --> Веб-безопасность** и указать необходимые параметры.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Записывать в журнал правил</b>	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
<b>Блокировать рекламу</b>	Активирует блокировку рекламы. Нажав на <b>Исключения</b> , администратор может выбрать URL-список сайтов, для которых блокировать рекламу не требуется.
<b>Инжектор</b>	Позволяет вставить произвольный код во все веб-страницы. Для редактирования вставляемого кода необходимо нажать на кнопку <b>Код инжектора</b> .
<b>Безопасный поиск</b>	Принудительно включает функцию безопасного поиска.
<b>История поиска</b>	Активирует запись поисковых запросов пользователей в журнал.
<b>Блокировать приложения социальных сетей</b>	Блокирует приложения в популярных социальных сетях.
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Пользователи</b>	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа <b>Any, Unknown, Known</b> . Для применения правил к конкретным пользователям или к пользователям типа <b>Known</b> необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе <a href="#">Пользователи и устройства</a> .
<b>Время</b>	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе <a href="#">Календари</a> .

## 8.3 Инспектирование SSL

С помощью данного раздела администратор может настроить инспекцию данных, передаваемых по протоколу TLS/SSL, это в первую очередь HTTPS, а также почтовые протоколы SMTPS и POP3S. В UserGate используется известная технология man-in-the-middle (MITM), при которой контент расшифровывается на сервере, а затем анализируется.

Инспектирование SSL необходимо для корректной работы правил фильтрации контента и правил веб-безопасности. Дешифрование SMTPS иPOP3S необходимо для блокирования спама и вирусной проверки почтового трафика.

С помощью правил данного раздела можно настроить инспектирование HTTPS только для определенных категорий, например, «Вредоносное ПО», «Анонимайзеры», «Ботнеты» и при этом не расшифровывать другие категории, например, «Финансы», «Правительство» и т.п. Для определения категории сайта используется информация, передаваемая в HTTPS-запросе - **SNI** (Server Name Indication), а если SNI отсутствует, то поле **Subject Name** в сертификате сервера. Содержимое поля **Subject Alternative Name** игнорируется.

После дешифрования данные шифруются сертификатом, выписанным центром сертификации, указанным в разделе **Сертификаты**. Чтобы браузеры пользователя не выдавали предупреждение о подмене сертификата, необходимо добавить сертификат центра сертификации в доверенные корневые сертификаты. Более подробно это описано в разделе [Управление сертификатами](#).

Аналогично браузерам пользователя некоторые почтовые серверы и пользовательские почтовые программы не принимают почту, если сертификат был подменен. В этом случае необходимо произвести в почтовых программах настройки, отключающие проверку сертификатов, или добавить исключения для сертификата UserGate. Подробно о том, как это сделать, смотрите в документации на почтовое ПО.

---

#### **Примечание**

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

---

#### **Примечание**

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

---

#### **Примечание**

Если не создано ни одного правила, то SSL не перехватывается и не дешифруются, соответственно, контент, передаваемый по SSL, не фильтруется.

---

## Примечание

UserGate поддерживает инспектирование широкого набора протоколов SSL, включая устаревшие версии, такие как TLSv1.0, TLSv1.1, и новые – TLSv1.2, TLSv1.3. По умолчанию включен режим совместимости с устаревшими протоколами, который обеспечивает поддержку набора TLSv1.0-TLSv1.2. При отключении режима совместимости с устаревшими протоколами поддерживается работа только TLSv1.0-TLSv1.3. Настройка производится с помощью команды CLI `legacy_ssl_enabled`, подробно о командах CLI смотрите раздел .

Чтобы создать правило инспектирования SSL, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности --> Инспектирование SSL** и указать необходимые параметры.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Записывать в журнал правил</b>	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.
<b>Действие</b>	Расшифровать Не расшифровывать
<b>Блокировать сайты с некорректными сертификатами</b>	Позволяет блокировать доступ к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат истек, отозван, выписан на другое доменное имя или не доверяемым центром сертификации.
<b>Проверять по списку отозванных сертификатов</b>	Проверять сертификат сайта в списке отозванных сертификатов (CRL) и блокировать, если он там найден.
<b>Блокировать сертификаты с истекшим сроком действия</b>	Блокировать сертификаты, срок действия которых истек.
<b>Блокировать самоподписанные сертификаты</b>	Блокировать самоподписанные сертификаты.
<b>Пользователи</b>	Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типа <b>Any, Unknown, Known</b> . Для применения правил к конкретным пользователям или к пользователям типа <b>Known</b> необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе <a href="#">Пользователи и устройства</a> .

<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Адрес назначения</b>	Списки IP-адресов назначения трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Сервис</b>	Сервис, для которого необходимо дешифровать трафик. Может быть HTTPS, SMTPS, POP3S.
<b>Категории</b>	Списки категорий UserGate URL filtering 4.0.
<b>Домены</b>	Списки доменов. Доменные имена, для которых применяется данное правило. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена ( <i>www.example.com</i> , а не <i>http://www.example.com/home/</i> ). Более подробно о работе со списками URL читайте в главе <a href="#">Списки URL</a> .
<b>Время</b>	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе <a href="#">Календари</a> .

По умолчанию создано правило инспектирования SSL **Decrypt all for unknown users**, которое необходимо для авторизации неизвестных пользователей через Captive-портал.

## 8.4 Система обнаружения и предотвращения вторжений

Система обнаружения и предотвращения вторжений (COB), или Intrusion Detection and Prevention System (IDPS), позволяет распознавать вредоносную активность внутри сети или со стороны интернета. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз, а также предоставление отчетов. Выявление проблем безопасности осуществляется с помощью использования эвристических правил и анализа сигнатур известных атак. База данных правил и сигнатур предоставляется и обновляется разработчиками UserGate при наличии соответствующей лицензии. COB отслеживает и блокирует подобные атаки в режиме реального времени. Возможными мерами превентивной защиты являются обрыв соединения, оповещение администратора сети и запись в журнал.

Для начала работы COB необходимо:

Наименование	Описание
<b>Шаг 1.</b> Создать необходимые профили COB	Профиль COB - это набор сигнатур, релевантных для защиты определенных сервисов. Администратор может создать необходимое количество профилей COB для защиты различных сервисов. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты сервиса. Например, для защиты сервиса, работающего по протоколу TCP, не стоит добавлять сигнатуры, разработанные для протокола UDP. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.
<b>Шаг 2.</b> Создать требуемые правила COB	Правила COB определяют действие COB для выбранного типа трафика, который будет проверяться модулем COB в соответствии с назначенными профилями COB.

Для настройки профилей COB необходимо создать профиль в разделе **Библиотеки --> Профили COB** и затем добавить в него необходимые сигнатуры. Сигнатуры COB поставляются и постоянно обновляются UserGate при наличии соответствующей подписки. Каждая сигнатура имеет определенные поля:

Наименование	Описание
<b>Сигнатура</b>	Название сигнатуры.
<b>Риск</b>	Риск сигнатуры по 5-бальной шкале
<b>Протокол</b>	<p>Протокол, для которого разработана данная сигнатура:</p> <ul style="list-style-type: none"> <li>• IP</li> <li>• ICMP</li> <li>• TCP</li> <li>• UDP</li> </ul>
<b>Категория</b>	<p>Категория сигнатуры - группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен.</p> <ul style="list-style-type: none"> <li>• attack_response - сигнатуры, определяющие ответы на известные сетевые атаки.</li> <li>• botcc - трафик, направленный к известным IP-адресам ботнетов.</li> <li>• botcc.portgrouped - трафик, направленный к известным IP-адресам и портам ботнетов.</li> <li>• ciarmy - трафик к топ-хакерам, определяемый командой www.ciarmy.com.</li> <li>• compromised - трафик к известным скомпрометированным хостам.</li> <li>• current_events - сигнатуры событий, вызываемых различными известными эксплоитами.</li> <li>• dns - известные уязвимости DNS.</li> <li>• dos - сигнатуры известных Denial of services атак.</li> <li>• drop - трафик к сетям, перечисленным в www.spamhaus.org.</li> <li>• dshield - трафик к топ-хакерам, определяемых командой www.dshield.org.</li> <li>• exploit - сигнатуры известных эксплоитов.</li> <li>• ftp - известные FTP-уязвимости.</li> <li>• icmp - известные ICMP-уязвимости.</li> <li>• icmp_info - ICMP-информация, потенциально предоставляющая излишнюю информацию.</li> <li>• imap - известные IMAP-уязвимости.</li> <li>• info - потенциальная утечка информации.</li> <li>• malware - скачивание, установка, деятельность известных malware.</li> <li>• misc - другие известные сигнатуры.</li> <li>• mobile_malware - сигнатуры известных malware для мобильных платформ.</li> <li>• netbios - известные уязвимости протокола NETBIOS.</li> <li>• p2p - сигнатуры протокола P2P.</li> <li>• policy - сигнатуры событий, потенциально нарушающие политику информационной безопасности (утечки информации).</li> <li>• pop3 - известные уязвимости протокола POP3.</li> <li>• rpc - известные уязвимости протокола RPC.</li> <li>• scada - известные уязвимости протокола SCADA.</li> <li>• scan - сигнатуры, определяющие попытки сканирования сети на известные приложения.</li> <li>• shellcode - сигнатуры, определяющие известные попытки запуска программных оболочек.</li> <li>• smtp - известные уязвимости протокола SMTP.</li> <li>• snmp - известные уязвимости протокола SNMP.</li> <li>• sql - известные уязвимости SQL.</li> <li>• telnet - известные попытки взлома по протоколу telnet.</li> </ul>

	<ul style="list-style-type: none"> <li>• tftp - известные уязвимости протокола TFTP.</li> <li>• tor - сигнатуры, определяющие tor-активность в сети.</li> <li>• trojan - сигнатуры известных троянов.</li> <li>• user_agents - сигнатуры подозрительных Useragent.</li> <li>• voip - известные уязвимости протокола VoIP.</li> <li>• web_client - сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player.</li> <li>• web_server - сигнатуры, определяющие известные попытки взлома различных веб-серверов.</li> <li>• web_specific_apps - сигнатуры, определяющие известные попытки взлома различных веб-приложений.</li> <li>• worm - сигнатуры, определяющие сетевую активность известных сетевых червей.</li> </ul>
<p><b>Класс</b></p>	<p>Класс сигнатуры определяет тип атаки, которая детектируется данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например, обнаружение установления сессии TCP. Поддерживаются следующие классы:</p> <ul style="list-style-type: none"> <li>• attempted-admin - попытка получения административных привилегий.</li> <li>• attempted-dos - попытка совершения атаки Denial of Service.</li> <li>• attempted-recon - попытка атаки, направленной на утечку данных.</li> <li>• attempted-user - попытка получения пользовательских привилегий.</li> <li>• bad-unknown - потенциально плохой трафик</li> <li>• default-login-attempt - попытка логина с именем/паролем по умолчанию.</li> <li>• denial-of-service - обнаружена атака Denial of Service.</li> <li>• misc-activity - прочая активность.</li> <li>• misc-attack - обнаружена атака.</li> <li>• network-scan - обнаружено сканирование сети.</li> <li>• non-standard-protocol - обнаружен нестандартный протокол.</li> <li>• not-suspicious - не подозрительный трафик.</li> <li>• policy-violation - потенциальное нарушение корпоративной политики ИБ.</li> <li>• protocol-command-decode - декодирована команда протокола.</li> <li>• rpc-portmap-decode - декодирован запрос RPC.</li> <li>• shellcode-detect - обнаружен исполняемый код.</li> <li>• string-detect - обнаружена подозрительная строка.</li> <li>• successful-admin - успешное получение административных привилегий.</li> <li>• successful-recon-largescale - утечка большого количества информации.</li> <li>• successful-recon-limited - утечка информации.</li> <li>• successful-user - успешное получение пользовательских привилегий.</li> <li>• suspicious-filename-detect - обнаружено подозрительное имя файла.</li> <li>• suspicious-login - попытка логина с использованием подозрительного имени пользователя.</li> <li>• system-call-detect - обнаружен системный вызов.</li> <li>• trojan-activity - обнаружен сетевой троян.</li> <li>• unsuccessful-user - неуспешная попытка получения пользовательских привилегий.</li> <li>• web-application-activity - обнаружен доступ к потенциально уязвимому веб-приложению.</li> <li>• web-application-attack - обнаружена атака на веб-приложение.</li> </ul>

При добавлении сигнатур в профиль SOB администратор может использовать гибкую возможность фильтрации сигнатур, например, выбрать только те сигнатуры, которые имеют очень высокий риск, протокол - TCP, категория - botcc, класс - все.

Правила SOB определяют трафик, к которому применяется профиль SOB и действие, которое модуль SOB должен предпринять при срабатывании сигнатуры.

### **Примечание**

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

### **Примечание**

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

### **Примечание**

Если не создано ни одного правила, то SOB ничего не анализирует и не защищает от угроз.

Для настройки правил SOB необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности --> SOB** и заполнить поля правила.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Действие</b>	Возможны следующие варианты: <ul style="list-style-type: none"><li>• <b>Разрешить</b> - не блокировать трафик.</li><li>• <b>Журналировать</b> - не блокировать и записать в журнал.</li><li>• <b>Запретить</b> - блокировать и записать в журнал.</li></ul>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .

<b>Назначение</b>	Зона назначения трафика и/или списки IP-адресов назначения трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Сервис</b>	Тип сервиса, например, HTTP, DNS или другие.
<b>Профили</b>	Список профилей COB, созданных на предыдущем шаге.

## 8.5 Правила АСУ ТП

С помощью правил АСУ ТП администратор может контролировать прохождение трафика автоматизированных систем управления технологическим производством (АСУ ТП) через UserGate. UserGate поддерживает контролирование следующих протоколов АСУ ТП:

- IEC 104 (ГОСТ Р МЭК 60870-5-104)
- Modbus
- DNP3
- MMS
- OPC UA

Администратору доступна возможность задать интересующие его профили АСУ ТП, в которых указать необходимый набор протоколов и команд, и использовать их в правилах.

Для начала работы с АСУ ТП необходимо:

Наименование	Описание
<b>Шаг 1.</b> Разрешить сервис SCADA на необходимой зоне	В разделе <b>Сеть --&gt; Зоны</b> разрешить сервис SCADA для той зоны, со стороны которой будет инициирован трафик АСУ ТП.
<b>Шаг 2.</b> Создать необходимые профили АСУ ТП	Профиль АСУ ТП - это набор элементов, каждый из которых состоит из определенной команды АСУ ТП и адреса.
<b>Шаг 3.</b> Создать требуемые правила АСУ ТП	Правила АСУ ТП определяют действие для выбранного типа трафика, который будет проверяться модулем АСУ ТП в соответствии с назначенными профилями.

Для настройки профилей АСУ ТП необходимо создать профиль в разделе **Библиотеки --> Профили АСУ ТП** и затем добавить в него необходимые команды. Каждая запись имеет определенные поля:

Наименование	Описание
<b>Название</b>	Название профиля.
<b>Описание</b>	Описание профиля.
<b>Записывать в журнал правил</b>	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.

<b>Протокол</b>	Выберите протокол АСУ ТП.
<b>Команда АСУ ТП</b>	Выберите необходимую команду АСУ ТП.
<b>Адрес АСУ ТП</b>	Укажите адрес АСУ ТП. Можно указать целое 4-байтовое число .

Правила АСУ ТП определяют трафик, к которому применяется профиль АСУ ТП и действие, которое UserGate должен предпринять при срабатывании правила.

### **Примечание**

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

### **Примечание**

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инvertировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Для создания правила АСУ ТП необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности -- > АСУ ТП** и заполнить поля правила.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Действие</b>	<p>Возможны следующие варианты:</p> <ul style="list-style-type: none"> <li>• <b>Пропускать</b> - не блокировать трафик.</li> <li>• <b>Блокировать</b> - блокировать и записать в журнал.</li> </ul> <p>Дополнительно можно выбрать опцию <b>Записывать в журнал правил</b>, в этом случае факт применения правила к трафику будет записан в соответствующий журнал.</p>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .

<b>Назначение</b>	Списки IP-адресов назначения трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Сервис</b>	Сервис L4, для которого будет действовать данное правило.
<b>Профили АСУ ТП</b>	Список профилей АСУ ТП, созданных на предыдущем шаге.

## 8.6 Сценарии

UserGate позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря концепции SOAR (Security Orchestration, Automation and Response). UserGate реализует данную концепцию с помощью механизма сценариев. Сценарий является дополнительным условием в правилах межсетевого экрана и в правилах пропускной способности, позволяя администратору настроить реакцию USERGATE на определенные события, произошедшие за некое продолжительное время. Примером работы сценариев могут являться решение следующих задач:

- Заблокировать или ограничить пропускную способность на 30 минут пользователя, у которого за последние 10 минут было обнаружено 5 попыток использования приложения torrent.
- Заблокировать или ограничить пропускную способность пользователя или группы пользователей, указанной в правиле, при срабатывании одного из следующих триггеров - открытие пользователем сайтов, относящихся к группе категорий Threats, срабатывание COB сигнатур высокого риска для трафика данного пользователя, блокировка вируса в трафике данного пользователя.
- Заблокировать или ограничить пропускную способность пользователя, если он выбрал лимит трафика в 10 Гб за месяц.



### Примечание

Сценарий является дополнительным условием в правилах межсетевого экрана и в правилах пропускной способности. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.

Для начала работы со сценариями необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать необходимые сценарии	В разделе <b>Политики безопасности --&gt; Сценарии</b> создать необходимые сценарии.
<b>Шаг 2.</b> Указать созданные сценарии в правилах межсетевого экрана или в правилах пропускной способности	Добавить созданный сценарий в правила межсетевого экрана или в правила пропускной способности. Более подробно о работе с правилами межсетевого экрана или пропускной способности смотрите раздел <a href="#">Политики сети</a> .

При создании сценария необходимо указать следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или отключает сценарий.
<b>Название</b>	Название сценария.
<b>Описание</b>	Описание сценария.
<b>Применить для</b>	Возможны варианты: <ul style="list-style-type: none"><li>• Одного пользователя - при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий.</li><li>• Всех пользователей - при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в поле Пользователи/Группы правила.</li></ul>
<b>Продолжительность</b>	Время в минутах, в течении которого сценарий будет активным после его активации. Столько же будет работать правило межсетевого экрана или пропускной способности, в котором используется данный сценарий.
<b>Условия</b>	Задаются условия срабатывания сценария. Для каждого условия можно указать количество срабатываний за определенное время, необходимое для срабатывания сценария. Если выбрано несколько условий, то необходимо указать, сработают ли сценарий при совпадении одного или всех условий.
<b>Условия срабатывания</b>	Возможны следующие условия для использования в сценарии: <ul style="list-style-type: none"><li>• Категория URL - совпадения указанных категорий UserGate URLF в трафике пользователя.</li><li>• Обнаружен вирус.</li><li>• Приложение - обнаружено указанное приложение в трафике пользователя.</li><li>• COB - сработка системы обнаружения вторжений.</li><li>• Типы контента - обнаружены указанные типы контента в трафике пользователя.</li><li>• Размер пакета - размер пакета в трафике пользователя превысил указанное значение.</li><li>• Сессий с одного IP - количество сессий с одного IP-адреса превысило указанное значение.</li><li>• Объем трафика - объем трафика пользователя превысил определенный лимит за указанную единицу времени.</li></ul>

## 8.7 Работа с внешними ICAP-серверами

UserGate позволяет передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. В данном случае UserGate будет выступать в роли ICAP-клиента.

UserGate поддерживает гибкие настройки при работе с ICAP-серверами, например, администратор может задать правила, согласно которым на ICAP-серверы будет направляться только выборочный трафик, или настроить работу с фермой ICAP-серверов.

Для того, чтобы настроить работу UserGate с внешними серверами ICAP, необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать ICAP-сервер	В разделе <b>Политики безопасности --&gt; ICAP-серверы</b> нажать на кнопку <b>Добавить</b> и создать один или более ICAP-серверов.
<b>Шаг 2.</b> Создать правило балансировки на ICAP-серверы (опционально)	В случае, если требуется балансировка на ферму ICAP-серверов, создать в разделе <b>Политики сети --&gt; Балансировка нагрузки</b> балансировщик ICAP-серверов. В качестве серверов используются ICAP-серверы, созданные на предыдущем шаге.
<b>Шаг 3.</b> Создать правило ICAP	В разделе <b>Политики безопасности --&gt; Правила ICAP</b> создать правило, которое будет задавать условия пересылки трафика на ICAP-серверы или фермы серверов.  Важно! Правила ICAP применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в настройках правила.

Для создания ICAP-сервера в разделе **Политики безопасности --> ICAP-серверы** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
<b>Название</b>	Название ICAP-сервера.
<b>Описание</b>	Описание ICAP-сервера.
<b>Адрес сервера</b>	IP-адрес ICAP-сервера.
<b>Порт</b>	TCP-порт ICAP-сервера, значение по умолчанию 1344.
<b>Максимальный размер сообщения</b>	Определяет максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. По умолчанию 0 (отключено).
<b>Период проверки доступности сервера ICAP</b>	Устанавливает время в секундах, через которое UserGate посылает OPTIONS-запрос на ICAP-сервер, чтобы убедиться, что сервер доступен.
<b>Пропускать при ошибках</b>	Если эта опция включена, то UserGate не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен (не отвечает на запрос OPTIONS).
<b>Reqmod путь</b>	<ul style="list-style-type: none"> <li>• <b>Вкл</b> - включает использование режима Reqmod.</li> <li>• <b>Путь на сервере ICAP для работы в режиме Reqmod.</b> Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах:</li> </ul>

	<ul style="list-style-type: none"> <li>• /path – путь на сервере ICAP;</li> <li>• <a href="#">icap://icap-server:port/path</a> – указание полного URI для режима reqmod.</li> </ul>
<b>Respmod путь</b>	<ul style="list-style-type: none"> <li>• <b>Вкл</b> - включает использование режима Reqmod.</li> <li>• <b>Путь на сервере ICAP для работы в режиме Respmod.</b> Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах:</li> <li>• /path – путь на сервере ICAP;</li> <li>• <a href="#">icap://icap-server:port/path</a> – указание полного URI для режима respmod.</li> </ul>
<b>Посылать имя пользователя</b>	<ul style="list-style-type: none"> <li>• <b>Вкл</b> - включает отсылку имени пользователя на ICAP-сервер.</li> <li>• <b>Кодировать в base64</b> - кодировать имя пользователя в base64, это может потребоваться, если имена пользователей содержат символы национальных алфавитов.</li> <li>• <b>Название заголовка</b>, которое будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию - X-Authenticated-User.</li> </ul>
<b>Посылать IP-адрес</b>	<ul style="list-style-type: none"> <li>• <b>Вкл</b> - включает отсылку IP-адреса пользователя на ICAP-сервер.</li> <li>• <b>Название заголовка</b>, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию - X-Client-Ip.</li> </ul>
<b>Посылать MAC-адрес</b>	<ul style="list-style-type: none"> <li>• <b>Вкл</b> - включает отсылку MAC-адреса пользователя на ICAP-сервер.</li> <li>• <b>Название заголовка</b>, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию - X-Client-Mac.</li> </ul>

Для создания правила балансировки на серверы ICAP в разделе **Политики сети --> Балансировка нагрузки** необходимо выбрать **Добавить --> Балансировщик ICAP** и заполнить следующие поля:

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>ICAP-серверы</b>	Список серверов ICAP, на которые будет распределяться нагрузка, созданный на предыдущем шаге.

Для создания ICAP-правила необходимо нажать **Добавить** в разделе **Политики безопасности --> ICAP-правила** и заполнить необходимые поля.

## Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже для изменения порядка применения правил.

## Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс Инvertировать в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Наименование	Описание
Вкл/Выкл	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Возможны следующие варианты: <ul style="list-style-type: none"><li>• <b>Пропустить</b> - не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP.</li><li>• <b>Переслать</b> - переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера. Это стандартный режим работы большинства ICAP-серверов.</li><li>• <b>Переслать и игнорировать</b> - переслать данные на ICAP-сервер и игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика.</li></ul>
ICAP-серверы	ICAP-сервер или балансировщик серверов ICAP, куда UserGate будет пересылать запросы.
Источник	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа <b>Any, Unknown, Known</b> . Для применения правил к конкретным пользователям или к пользователям типа <b>Known</b> необходимо настроить идентификацию пользователей.

<b>Адрес назначения</b>	IP-адреса, GeoIP или списки URL (хостов) назначения трафика.
<b>Типы контента</b>	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе <a href="#">Типы контента</a> .
<b>Категории</b>	Списки категорий UserGate URL filtering.
<b>URL</b>	Списки URL.
<b>HTTP метод</b>	Метод, используемый в HTTP-запросах, как правило, это POST или GET.
<b>Сервис</b>	<p>Возможны варианты:</p> <ul style="list-style-type: none"> <li>• <b>HTTP</b> - веб-трафик.</li> <li>• <b>SMTP</b> - почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа.</li> <li>• <b>POP3</b> - почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа.</li> </ul> <p>Важно! Перед использованием сервисов SMTP и POP3 в правилах ICAP необходимо создать правило защиты почтового трафика для данных сервисов. Подробнее о защите почтового трафика смотрите в разделе <a href="#">Защита почтового трафика</a>.</p>

## 8.8 Защита почтового трафика

Раздел **Защита почтового трафика** позволяет настроить проверку транзитного почтового трафика на предмет наличия в нем вирусов и спам-сообщений. Поддерживается работа с почтовыми протоколами POP3(S) и SMTP(S). Защита почтового трафика требует наличия соответствующего модуля в лицензии UserGate.

Как правило, необходимо защищать почтовый трафик, входящий из интернета на внутренние почтовые серверы компании, и, в некоторых случаях, защищать исходящий почтовый трафик от серверов или пользовательских компьютеров.

Для защиты почтового трафика, приходящего из интернета на внутренние почтовые серверы, необходимо:

Наименование	Описание
<b>Шаг 1.</b> Опубликовать почтовый сервер в сеть Интернет	Смотрите раздел <b>Правила DNAT</b> . Рекомендуется создать отдельные правила DNAT для SMTP и POP3 протоколов, а не публиковать оба протокола в одном правиле. Обязательно укажите в качестве сервиса протокола SMTP, а не TCP.
<b>Шаг 2.</b> Включить поддержку сервисов SMTP(S) и POP3(S) в зоне, подключенной к сети Интернет	Смотрите раздел <b>Настройка зон</b> .

<b>Шаг 3.</b> Создать правила защиты почтового трафика	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.
--	---

Для защиты почтового трафика в случаях, когда не требуется публиковать почтовый сервер, действия сводятся к следующим шагам:

Наименование	Описание
<b>Шаг 1.</b> Создать правила защиты почтового трафика	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Для настройки правил фильтрации почтового трафика необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности --> Защита почтового трафика** и заполнить поля правила.

### **Примечание**

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

### **Примечание**

Если не создано ни одного правила, то почтовый трафик не проверяется.

### **Примечание**

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.

<b>Описание</b>	Описание правила.
<b>Действие</b>	<p>Действие, применяемое к почтовому трафику при совпадении всех условий правила:</p> <ul style="list-style-type: none"> <li>• <b>Пропустить</b> - пропускает трафик без изменений.</li> <li>• <b>Маркировать</b> - маркирует почтовые сообщения специальным тэгом в теме письма или дополнительном поле.</li> <li>• <b>Блокировать с ошибкой</b> - блокирует письмо, при этом сообщает об ошибке доставки письма серверу SMTP для SMTP(S)-трафика или клиенту POP3 для POP3(S)-трафика.</li> <li>• <b>Блокировать без ошибки</b> - блокирует письмо без уведомления о блокировке.</li> </ul>
<b>Проверка</b>	<p>Метод проверки почтового трафика:</p> <ul style="list-style-type: none"> <li>• <b>Проверка антиспамом UserGate</b> - проверяет почтовый трафик на наличие спама.</li> <li>• <b>DNSBL проверка</b> - антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам и вирусы.</li> </ul>
<b>Заголовок</b>	Поле, куда помещать тег маркировки.
<b>Маркировка</b>	Текст тега, который маркирует письмо.
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Назначение</b>	IP-адреса, GeoIP или списки URL (хостов) назначения трафика.
<b>Пользователи</b>	Пользователи или группы пользователей, к которым применяется данное правило.
<b>Сервис</b>	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило.
<b>Envelop from</b>	Почтовый адрес отправителя письма, указанный в поле <b>Envelop from</b> . Только для протокола SMTP.
<b>Envelop to</b>	Почтовый адрес адресата письма, указанный в поле <b>Envelop to</b> . Только для протокола SMTP.

Рекомендуемые настройки защиты от спама следующие.

Для протокола SMTP(S):

- Первое правило в списке - **блокировка с помощью DNSBL**. Рекомендуется оставить списки **Envelop from/Envelop to** пустыми. В этом случае DNSBL будет отбрасывать подключения SMTP-серверов, замеченных в распространении спама, еще на этапе коннекта. При наличии e-mail адресатов в этих списках система будет вынуждена принимать сообщения целиком для анализа этих полей, что увеличит нагрузку на сервер и ухудшит производительность проверки почтового трафика.
- Второе правило - **маркировка** писем с помощью антиспама UserGate. Здесь можно использовать любые исключения, в том числе и по **Envelop from/Envelop to**.

Для протокола POP3(S):

- Действие - **Маркировать**.

- Проверка - **Антиспам UserGate**.

## 8.9 Защита от DoS атак

UserGate позволяет гранулированно настроить параметры защиты сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP). Грубая настройка производится в свойствах зон (смотрите раздел [Настройка зон](#)), более точная настройка производится в данном разделе. Используя правила защиты DoS, администратор может указать специфические настройки защиты от DoS атак для определенного сервиса, протокола, приложения и т.п. Чтобы создать правила защиты DoS администратору необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать профили DoS защиты	В разделе <b>Политики безопасности</b> --> <b>Профили DoS</b> нажать на кнопку <b>Добавить</b> и создать один или более профилей DoS защиты.
<b>Шаг 2.</b> Создать правила защиты DoS	В разделе <b>Политики безопасности</b> --> <b>Правила защиты DoS</b> создайте правила, используя профили защиты, созданные на предыдущем шаге.

Настройка профиля защиты DoS подобна настройке защиты от DoS на зонах UserGate. При создании профиля необходимо указать следующие параметры:

Наименование	Описание
<b>Название</b>	Название профиля.
<b>Описание</b>	Описание профиля.
<b>Агрегировать</b>	Данная настройка регулирует, будет ли UserGate суммировать количество пакетов, проходящих в секунду, для всех IP-адресов источника трафика, или будет производить подсчет индивидуально для каждого IP-адреса. В случае активации данной настройки необходимо устанавливать достаточно высокие значения количества пакетов/сек в настройках закладки <b>Защита DoS</b> и в закладке <b>Защита ресурсов</b> .
<b>Защита DoS</b>	Данная настройка позволяет указать параметры защиты от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: <ul style="list-style-type: none"> <li>• <b>Порог уведомления</b> - при превышении количества запросов над указанным значением происходит запись события в системный журнал.</li> <li>• <b>Порог отбрасывания пакетов</b> - при превышении количества запросов над указанным значением UserGate начинает отбрасывать пакеты, и записывает данное событие в системный журнал.</li> </ul>
<b>Защита ресурсов</b>	Данная настройка позволяет ограничить количество сессий, которые будут разрешены для защищаемого ресурса, например, опубликованного сервера: <ul style="list-style-type: none"> <li>• <b>Вкл</b> - включает ограничение количества сессий.</li> <li>• <b>Ограничить число сессий</b> - задается число сессий.</li> </ul>

Чтобы создать правило защиты DoS, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности** --> **Правила защиты DoS** и указать необходимые параметры.

### **Примечание**

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже** для изменения порядка применения правил.

### **Примечание**

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Действие</b>	<b>Запретить</b> - безусловно блокирует трафик подобно действию правил Межсетевого экрана. <b>Разрешить</b> - разрешает трафик, защита от DoS не применяется. Может быть использовано для создания исключений. <b>Защитить</b> - применить профиль защиты от DoS атак.
<b>Профиль DoS</b>	В случае, если выбрано действие Защитить, необходимо указать профиль защиты DoS.
<b>Сценарий</b>	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе <a href="#">Сценарии</a> . Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
<b>Записывать в журнал правил</b>	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: <ul style="list-style-type: none"><li>Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.</li></ul>

	<ul style="list-style-type: none"> <li>Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.</li> </ul>
<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика.
<b>Пользователи</b>	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа <b>Any, Unknown, Known</b> . Для применения правил к конкретным пользователям или к пользователям типа <b>Known</b> необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе <a href="#">Пользователи и устройства</a> .
<b>Назначение</b>	Зона назначения трафика и/или списки IP-адресов назначения трафика.
<b>Сервис</b>	Тип сервиса, например, HTTP или HTTPS.
<b>Время</b>	Интервалы времени, когда правило активно.

## 9 ГЛОБАЛЬНЫЙ ПОРТАЛ

Веб-портал и reverse-прокси, наряду с правилами DNAT/Порт-форвардинга, позволяют опубликовать ресурсы, находящиеся внутри компании, пользователям из интернета.

При наличии публикаций внутренних ресурсов с помощью DNAT/Порт-форвардинга, Reverse-прокси и веб-портала порядок обработки правил следующий:

1. Правила DNAT.
2. Правила веб-портала. Если имя хоста в запросе совпало с именем хоста веб-портала, то обрабатывают правила веб-портала.
3. Правила Reverse-прокси.

### 9.1 Веб-портал (SSL VPN)

Веб-портал позволяет предоставить доступ к внутренним веб-ресурсам, терминальным и ssh-серверам компании для удаленных или мобильных пользователей, используя при этом только протокол HTTPS. Данная технология не требует установки специального клиента VPN, достаточно обычного браузера.

Для настройки веб-портала необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Включить и настроить веб-портал	В разделе <b>Настройки --&gt; Веб-портал</b> включить и настроить параметры веб-портала. Подробные значения настроек будут описаны далее в этой главе.
<b>Шаг 2.</b> Разрешить доступ к сервису веб-портала на необходимых зонах	В разделе <b>Сеть --&gt; Зоны</b> разрешить сервис веб-портала для выбранных зон (обычно зона Untrusted). Данное разрешение откроет доступ к порту сервиса, который был указан в настройках веб-портала на предыдущем шаге.
<b>Шаг 3.</b> Добавить внутренние ресурсы в веб-портал	В разделе <b>Глобальный портал --&gt; Веб-портал</b> добавить URL внутренних ресурсов, к которым необходим доступ пользователей. Подробные значения настроек будут описаны далее в этой главе.

При настройке веб-портала (раздел **Настройки --> Веб-портал**) необходимо заполнить следующие поля:

Наименование	Описание
<b>Вкл</b>	Включает/Выключает веб-портал.
<b>Имя хоста</b>	Имя хоста, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. Данное имя должно резолвиться службами DNS в IP-адрес интерфейса UserGate, входящего в зону, на которой разрешен сервис веб-портала .
<b>Порт</b>	Порт TCP, который будет использоваться сервисом веб-портала. Порт вместе с именем хоста образуют URL для подключения пользователей в виде:

	<a href="https://имя_хоста:порт.">https://имя_хоста:порт.</a>
<b>Профиль авторизации</b>	<p>Профиль авторизации пользователей, который будет использоваться для авторизации пользователей, подключающихся к веб-порталу. Профиль авторизации задает метод авторизации, например, AD-коннектор или локальный пользователь. Также в профиле авторизации можно указать требование использовать мультифакторную авторизацию для доступа к веб-порталу.</p> <p>Более подробно о профилях авторизации смотрите раздел руководства <a href="#">Профили авторизации</a>.</p>
<b>Шаблон страницы авторизации</b>	<p>Выбрать шаблон страницы авторизации, который будет использоваться для отображения формы для ввода логина и пароля. Создать свою страницу авторизации можно в разделе <a href="#">Шаблоны страниц</a>.</p>
<b>Шаблон портала</b>	<p>Выбрать шаблон веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Создать свою страницу авторизации можно в разделе <a href="#">Шаблоны страниц</a>.</p>
<b>Предлагать выбор домена AD/LDAP на странице авторизации</b>	<p>Показывать выбор домена на странице авторизации веб-портала.</p>
<b>Показывать CAPTCHA</b>	<p>При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице авторизации веб-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.</p>
<b>Сертификат</b>	<p>Сертификат, который будет использоваться для создания HTTPS-соединения. Если выбран режим <b>Автоматически</b>, то используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Более подробно о ролях сертификатов смотрите в разделе руководства <a href="#">Управление сертификатами</a>.</p>
<b>Авторизация пользователя по сертификату</b>	<p>Если выбрано, то требует предъявления пользовательского сертификата браузером. Для этого пользовательский сертификат должен быть добавлен в список сертификатов UserGate, ему должна быть назначена роль <b>Пользовательский сертификат</b> и назначен соответствующий пользователь UserGate. Более подробно о пользовательских сертификатах читайте в разделе <a href="#">Управление сертификатами</a>.</p>

Настройке веб-портала (раздел **Глобальный портал --> Веб портал**) сводится к тому, что необходимо создать записи публикации URL внутренних веб-ресурсов. Для каждого URL необходимо создать закладку и заполнить следующие поля:

Наименование	Описание
<b>Вкл</b>	Включает или отключает закладку.
<b>Название</b>	Название закладки.
<b>Описание</b>	Описание закладки.

<b>URL</b>	<p>URL ресурса, который необходимо опубликовать через веб-портал. Указывайте полный URL, начиная с <b>Ошибка! Недопустимый объект гиперссылки., Ошибка! Недопустимый объект гиперссылки., Ошибка! Недопустимый объект гиперссылки.</b> или <code>gdp://</code></p> <p>Важно! Для публикации терминальных серверов необходимо отключить опцию, требующую Network Level Authentication в свойствах RDP доступа на серверах терминального доступа. Аутентификацию пользователей для доступа к серверам в данном случае будет выполнять веб-портал в соответствии со своими настройками.</p>
<b>Домен прямого доступа</b>	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену.
<b>Иконка</b>	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из predefined иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку.
<b>Вспомогательные URL</b>	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Например, основной URL <a href="http://www.example.com">http://www.example.com</a> получает часть медиаконтента со вспомогательного URL <a href="http://cdn.example.com">http://cdn.example.com</a> .
<b>Пользователи</b>	Список пользователей и/или групп пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL.

Очередность закладок в веб-портала определяет порядок отображения их пользователю. Администратор может менять очередность закладок с помощью кнопок **Наверх, Выше, Ниже, Вниз** или перетаскивая закладки с помощью мыши.

## 9.2 Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси

Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси.

В отличие от публикации с помощью правил DNAT, публикация с использованием reverse-прокси предоставляет следующие преимущества:

- Публикация по HTTPS серверов, работающих по HTTP и наоборот.
- Балансировка запросов на ферму веб-серверов.
- Возможность ограничения доступа к публикуемым серверам с определенных Useragent.
- Возможность подмены доменов и путей публикуемых серверов.

Чтобы опубликовать сервер, используя reverse-прокси, необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать сервер reverse-прокси	В разделе <b>Глобальный портал --&gt; Серверы reverse-прокси</b> нажать на кнопку <b>Добавить</b> и создать один или более публикуемых веб-серверов.
<b>Шаг 2.</b> Создать правило балансировки на серверы reverse-прокси	В случае, если требуется балансировка на ферму публикуемых серверов, создать в разделе <b>Политики сети --&gt; Балансировка нагрузки</b>

(опционально)	балансировщик reverse-прокси. В качестве серверов используются серверы reverse-прокси, созданные на предыдущем шаге.
<b>Шаг 3.</b> Создать правило reverse-прокси	В разделе <b>Глобальный портал --&gt; Правила reverse-прокси</b> создать правило, которое будет задавать условия публикации серверов или фермы серверов.  Важно! Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в настройках правила.
<b>Шаг 4.</b> Разрешить сервис Reverse-прокси на зоне, с которой необходимо разрешить доступ к внутренним ресурсам	В разделе <b>Сеть --&gt; Зоны</b> разрешите сервис Reverse-прокси для зоны, с которой необходимо разрешить доступ к внутренним ресурсам (обычно зона Untrusted).

Для создания сервера reverse-прокси разделе **Глобальный портал --> Серверы reverse-прокси** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
<b>Название</b>	Название публикуемого сервера.
<b>Описание</b>	Описание публикуемого сервера.
<b>Адрес сервера</b>	IP-адрес публикуемого сервера.
<b>Порт</b>	TCP-порт публикуемого сервера.
<b>HTTPS до сервера</b>	Определяет, требуется ли использовать протокол HTTPS до публикуемого сервера.
<b>Проверять SSL-сертификат</b>	Включает/отключает проверку валидности SSL-сертификата, установленного на публикуемом сервере.
<b>Не изменять IP-адрес источника</b>	Оставляет оригинальный IP-адрес источника в пакетах, пересылаемых на публикуемый сервер. Если отключено, то IP-адрес источника заменяется на IP-адрес UserGate.

Для создания правила балансировки на серверы reverse-прокси в разделе **Политики сети --> Балансировка нагрузки** необходимо выбрать **Добавить --> Балансировщик reverse-прокси** и заполнить следующие поля:

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Серверы reverse-</b>	Созданный на предыдущем шаге список серверов reverse-прокси, на которые будет

Для создания правила reverse-прокси необходимо нажать на кнопку **Добавить** в разделе **Глобальный портал** --> **Правила reverse-прокси** и заполнить необходимые поля.

### Примечание

Правила применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Вверх/Вниз для изменения порядка применения правил.

### Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила. Чекбокс **Инвертировать** в условии правила меняет действие условия на противоположное, что аналогично логическому действию отрицание.

Наименование	Описание
<b>Вкл/Выкл</b>	Включает или отключает правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Сервер reverse-прокси</b>	Сервер reverse-прокси или балансировщик reverse-прокси, куда UserGate будет пересылать запросы.
<b>Порт</b>	Порт, на котором UserGate будет слушать входящие запросы.
<b>Использовать HTTPS</b>	Включает поддержку HTTPS.
<b>Сертификат</b>	Сертификат, используемый для поддержки HTTPS-соединения.
<b>Авторизовать по сертификату</b>	Если выбрано, то требует предъявления пользовательского сертификата браузером. Для этого пользовательский сертификат должен быть добавлен в список сертификатов UserGate, ему должна быть назначена роль <b>Пользовательский сертификат</b> и назначен соответствующий пользователь UserGate. Более подробно о пользовательских сертификатах читайте в разделе <a href="#">Управление сертификатами</a> .

<b>Источник</b>	Зона источника трафика и/или списки IP-адресов источника трафика. Более подробно о работе со списками IP-адресов читайте в главе <a href="#">IP-адреса</a> .
<b>Пользователи</b>	<p>Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типа <b>Any, Unknown, Known</b>. Для применения правил к конкретным пользователям или к пользователям типа <b>Known</b> необходимо настроить идентификацию пользователей.</p> <p>Данная вкладка доступна только при использовании HTTPS и авторизации пользователя по сертификату.</p>
<b>Назначение</b>	Один из внешних IP-адресов сервера UserGate, доступный из сети интернет, куда адресован трафик внешних клиентов.
<b>Useragent</b>	UserAgent пользовательских браузеров, для которых будет применено данное правило.
<b>Подмена путей</b>	<p>Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на <a href="http://www.example.com/path1">http://www.example.com/path1</a> в <a href="http://www.example.loc/path2">http://www.example.loc/path2</a></p> <p>Изменить с - домен и/или путь URL, которые требуется изменить.</p> <p>Изменить на - домен и/или путь URL, на которые требуется заменить старые.</p> <p>Если указан домен в поле <b>Изменить с</b>, то правило публикации будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.</p>

## 10 НАСТРОЙКА VPN

VPN ([Virtual Private Network](#) - виртуальная частная сеть) - обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, [интернет](#)). UserGate позволяет создавать VPN-подключения следующих типов:

- VPN-сервер для удаленного доступа клиентов (Remote access VPN). В данном случае UserGate выступает в качестве сервера, а пользователи других устройств выступают в качестве клиентов VPN. UserGate поддерживает работу со стандартными клиентами большинства популярных операционных систем, например, таких, как Windows, Linux, Mac OS X, iOS, Android и другие.
- VPN для защищенного соединения офисов (Site-to-Site VPN). В данном случае один сервер UserGate выступает в качестве сервера, а другой UserGate-сервер выступает в роли клиента. Клиент инициирует соединение с сервером. Подключение сервер-сервер позволяет объединить разобщенные офисы компании в единую логическую сеть.

Для создания туннелей используется протокол Layer 2 Tunneling Protocol (L2TP), а для защиты передаваемых данных - протокол IPSec. Поддерживается многофакторная авторизация пользователей при подключении к сервису VPN.

### 10.1 VPN для удаленного доступа клиентов (Remote access VPN)

Для подключения VPN-клиентов к корпоративной сети необходимо настроить UserGate для выполнения роли VPN-сервера. Для этого необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты	В разделе <b>Сеть --&gt; Зоны</b> отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервис VPN. Как правило, это зона <b>Untrusted</b> .
<b>Шаг 2.</b> Создать зону, в которую будут помещены подключаемые по VPN клиенты	В разделе <b>Сеть --&gt; Зоны</b> создать зону, в которую будут помещены подключаемые по VPN клиенты. Эту зону в дальнейшем можно использовать в политиках безопасности.  Рекомендуется использовать уже существующую по умолчанию зону <b>VPN for remote access</b> .
<b>Шаг 3.</b> Создать правило NAT для созданной зоны	Клиенты подключаются к VPN с использованием Point-to-Point протокола. Чтобы трафик мог ходить из созданной на предыдущем шаге зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Создайте соответствующее правило в разделе <b>Политики сети --&gt; NAT и маршрутизация</b> .  По умолчанию в UserGate создано правило <b>NAT from VPN for remote access to Trusted and Untrusted</b> , разрешающее наттирование из зоны <b>VPN for remote access</b> в зоны <b>Trusted</b> и <b>Untrusted</b> .
<b>Шаг 4.</b> Создать разрешающее правило межсетевого экрана для трафика из созданной зоны	В разделе <b>Политики сети --&gt; Межсетевой экран</b> создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны.  По умолчанию в UserGate создано правило межсетевого экрана <b>VPN for remote access</b>

	<p><b>to Trusted and Untrusted</b>, разрешающее весь трафик из <b>зоны VPN for remote access</b> в зоны <b>Trusted</b> и <b>Untrusted</b>.</p>
<p><b>Шаг 5.</b> Создать профиль авторизации</p>	<p>В разделе <b>Пользователи и устройства --&gt; Профили авторизации</b> создать профиль авторизации для пользователей VPN. Допускается использовать тот же профиль авторизации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной авторизации, такие как Kerberos, NTLM, SAML IDP.</p> <p>VPN поддерживает многофакторную авторизацию. Вторым фактором авторизации может быть получен через одноразовые коды TOTP, sms или e-mail. Для ввода второго фактора авторизации пользователь при подключении к VPN серверу должен указать свой пароль в виде:</p> <p><i>пароль:одноразовый_код</i></p> <p>где <i>пароль</i> - это пароль пользователя</p> <p>: - разделитель</p> <p><i>одноразовый_код</i> - второй фактор авторизации.</p> <p>Подробнее о профилях авторизации смотрите в разделе данного руководства <a href="#">Профили авторизации</a>.</p>
<p><b>Шаг 6.</b> Создать профиль безопасности VPN</p>	<p>Профиль безопасности VPN определяет такие настройки, как общий ключ шифрования (Preshared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей и использовать их для построения соединений с разными типами клиентов.</p> <p>Для создания профиля необходимо перейти в раздел <b>VPN --&gt; Профили безопасности VPN</b>, нажать кнопку <b>Добавить</b> и заполнить следующие поля:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> - название профиля.</li> <li>• <b>Описание</b> - описание профиля.</li> <li>• <b>Общий ключ</b> - строка, которая должна совпадать на сервере и клиенте для успешного подключения.</li> <li>• <b>Безопасность --&gt; Методы шифрования</b> - пары алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, в котором они изображены (сверху вниз). При установлении соединения используется первая пара, которую поддерживают сервер и клиент. Для совместимости со стандартными клиентами VPN рекомендуется оставить значения по умолчанию.</li> </ul> <p>По умолчанию в UserGate создан серверный профиль <b>Remote access VPN profile</b>, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, то необходимо изменить общий ключ шифрования.</p>
<p><b>Шаг 7.</b> Создать VPN-интерфейс</p>	<p>VPN-интерфейс – это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.</p> <p>В разделе <b>Сеть --&gt; Интерфейсы</b> нажмите кнопку <b>Добавить</b>, и выберите <b>Добавить VPN</b>.</p>

	<p>Задайте следующие параметры:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> – название интерфейса, должно быть в виде tunnelN, где N – это порядковый номер VPN-интерфейса.</li> <li>• <b>Описание</b> – описание интерфейса.</li> <li>• <b>Зона</b> – зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к серверу UserGate будут так же помещены в эту зону. Укажите зону, созданную на шаге 2.</li> <li>• <b>Профиль Netflow</b> – профиль Netflow, используемый для данного интерфейса. Не обязательный параметр.</li> <li>• <b>Режим</b> - тип присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN, то необходимо использовать статический IP-адрес.</li> <li>• <b>MTU</b> – размер MTU для выбранного интерфейса.</li> </ul> <p>По умолчанию в системе уже создан VPN-интерфейс <b>tunnel1</b>, который рекомендовано использовать для Remote access VPN.</p>
<p><b>Шаг 8.</b> Создать сеть VPN</p>	<p>VPN-сеть определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и - опционально - маршруты, которые будут переданы клиентам для применения, если клиенты поддерживает применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов.</p> <p>Для создания туннеля VPN перейдите в раздел <b>VPN --&gt; Сети VPN</b>, нажмите кнопку <b>Добавить</b> и заполните следующие поля:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> - название сети.</li> <li>• <b>Описание</b> - описание сети.</li> <li>• <b>Диапазон IP-адресов</b>, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемым совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.</li> <li>• Укажите <b>DNS-сервера</b>, которые будут переданы клиенту, или поставьте галочку <b>Использовать системные DNS</b>, в этом случае клиенту будут назначены DNS-серверы, которые использует UserGate.</li> <li>• Укажите <b>маршруты</b>, передаваемые клиенту в виде бесклассовой адресации (CIDR)</li> </ul> <p>В UserGate создана сеть <b>Remote access VPN network</b> с рекомендуемыми настройками.</p>
<p><b>Шаг 9.</b> Создать серверное правило VPN</p>	<p>Создать серверное правило VPN, используя в нем созданные ранее сеть VPN, интерфейс VPN и профиль VPN. Для создания правила необходимо перейти в раздел <b>VPN --&gt; Серверные правила</b>, нажать кнопку <b>Добавить</b> и заполнить следующие поля:</p> <ul style="list-style-type: none"> <li>• <b>Вкл/Выкл</b> - включает/отключает правило.</li> <li>• <b>Название</b> - название правила.</li> <li>• <b>Описание</b> - описание правила.</li> <li>• <b>Профиль безопасности</b> - профиль безопасности, созданный ранее.</li> <li>• <b>Сеть VPN</b> - сеть VPN, созданная ранее.</li> <li>• <b>Профиль авторизации</b> - профиль авторизации, созданный ранее.</li> <li>• <b>URL инициализации TOTP</b> - url, по которому пользователь может провести</li> </ul>

	<p>первоначальную инициализацию своего TOTP-устройства, в случае, если настроена многофакторная авторизация TOTP для авторизации VPN.</p> <ul style="list-style-type: none"> <li>• <b>Интерфейс</b> - интерфейс VPN, созданный ранее.</li> <li>• <b>Источник</b> - зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону <b>Untrusted</b>.</li> <li>• <b>Пользователи</b> - группа пользователей или отдельные пользователи, которым разрешено подключаться по VPN.</li> </ul> <p>По умолчанию в UserGate создано серверное правило <b>Remote access VPN rule</b>, в котором используются необходимые настройки для <b>Remote Access VPN</b>, а доступ к VPN разрешен членам локальной группы <b>VPN users</b>.</p> <p>Важно! Для применения различных серверных правил к разным клиентам необходимо использовать параметры <b>Исходная зона</b> и <b>Адрес источника</b>. Параметр <b>Пользователь</b> не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.</p>
<p><b>Шаг 10.</b> Настроить VPN на клиентском компьютере</p>	<p>Для настройки клиентского подключения к VPN на компьютере пользователя необходимо указать следующие параметры:</p> <ul style="list-style-type: none"> <li>• Используйте тип подключения VPN - L2TP over IPSec.</li> <li>• В качестве IP-адреса VPN-сервера укажите IP-адрес интерфейса зоны, указанной на шаге 1.</li> <li>• В качестве общего ключа (Preshared key, Shared secret) используйте общий ключ, указанный вами на шаге 6.</li> <li>• Укажите протокол PAP для авторизации пользователя.</li> <li>• В качестве имени пользователя укажите имя учетной записи пользователя в формате <a href="#">username@domain</a>, например, <a href="#">testuser@testdomain.loc</a></li> </ul> <p>Важно! Операционные системы Microsoft Windows требуют изменения параметров реестра для корректной работы с VPN-сервером L2TP/IPSec. Обратитесь к статье Microsoft <a href="https://support.microsoft.com/en-us/help/926179/how-to-configure-an-l2tp-ipsec-server-behind-a-nat-t-device-in-windows">https://support.microsoft.com/en-us/help/926179/how-to-configure-an-l2tp-ipsec-server-behind-a-nat-t-device-in-windows</a> за подробной инструкцией.</p>

## 10.2 VPN для защищенного соединения офисов (Site-to-Site VPN)

Для создания Site-to-Site VPN необходимо настроить один UserGate для выполнения роли VPN-клиента, а другой - для выполнения роли VPN-сервера. Хотя настройка UserGate для выполнения роли VPN-сервера близка к настройке сервера для удаленного доступа, мы рекомендуем произвести все настройки отдельно, поскольку часть настроек может отличаться.

Настройка сервера, выполняющего роль VPN-сервера для объединения офисов:

Наименование	Описание
<p><b>Шаг 1.</b> Создать локального пользователя для авторизации сервера, выступающего в роли VPN-клиента</p>	<p>В разделе <b>Пользователи и устройства --&gt; Пользователи</b> создать пользователей для каждого из удаленных UserGate-серверов, выступающих в роли VPN-клиентов, задать пароли. Рекомендуется поместить всех созданных пользователей в группу, которой будет дан доступ для подключения по VPN. По умолчанию для этой цели в UserGate создана группа <b>VPN servers</b>.</p>

<p><b>Шаг 2.</b> Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты</p>	<p>В разделе <b>Сеть --&gt; Зоны</b> отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервис VPN. Как правило, это зона <b>Untrusted</b>.</p>
<p><b>Шаг 3.</b> Создать зону, в которую будут помещены подключаемые по VPN серверы</p>	<p>В разделе <b>Сеть --&gt; Зоны</b> создать зону, в которую будут помещены подключаемые по VPN серверы. Эту зону в дальнейшем можно будет использовать в политиках безопасности.</p> <p>Рекомендуется использовать уже существующую по умолчанию зону <b>VPN for Site-to-Site</b>.</p>
<p><b>Шаг 4.</b> Создать разрешающее правило межсетевого экрана для трафика из созданной зоны</p>	<p>В разделе <b>Политики сети --&gt; Межсетевой экран</b> создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны.</p> <p>По умолчанию в UserGate создано правило межсетевого экрана <b>VPN for Site-to-Site to Trusted and Untrusted</b>, разрешающее весь трафик из зоны <b>VPN for Site-to-Site в Trusted и Untrusted</b> зоны. Правило выключено по умолчанию.</p>
<p><b>Шаг 5.</b> Создать профиль авторизации</p>	<p>В разделе <b>Пользователи и устройства --&gt; Профили авторизации</b> создать профиль авторизации для пользователей VPN. Допускается использовать тот же профиль авторизации, что используется для авторизации пользователей, для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной авторизации, такие как Kerberos, NTLM, SAML IDP.</p> <p>Подробно о профилях авторизации смотрите в разделе данного руководства <a href="#">Профили авторизации</a>.</p>
<p><b>Шаг 6.</b> Создать профиль безопасности VPN</p>	<p>Профиль безопасности определяет такие настройки, как общий ключ шифрования (Preshared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов.</p> <p>Для создания профиля безопасности необходимо перейти в раздел <b>VPN --&gt; Профили безопасности</b>, нажать кнопку <b>Добавить</b> и заполнить следующие поля:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> - название профиля.</li> <li>• <b>Описание</b> - описание профиля.</li> <li>• <b>Общий ключ</b> - строка, которая должна совпадать на сервере и клиенте для успешного подключения.</li> <li>• <b>Безопасность --&gt; Методы шифрования</b> - пары алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, в котором они изображены (сверху вниз). При установлении соединения используется первая пара, которую поддерживают сервер и клиент. Для совместимости со стандартными клиентами VPN рекомендуется оставить значения по умолчанию.</li> </ul> <p>По умолчанию в UserGate создан профиль безопасности <b>Site-to-Site VPN profile</b>, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, необходимо изменить общий ключ шифрования.</p>
<p><b>Шаг 7.</b> Создать VPN-интерфейс</p>	<p>VPN-интерфейс – это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут</p>

	<p>автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.</p> <p>В разделе <b>Сеть --&gt; Интерфейсы</b> нажмите кнопку <b>Добавить</b>, и выберите <b>Добавить VPN</b>. Задайте следующие параметры:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> – название интерфейса, должно быть в виде tunnelN, где N – это порядковый номер VPN-интерфейса.</li> <li>• <b>Описание</b> – описание интерфейса.</li> <li>• <b>Зона</b> – зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к серверу UserGate будут так же помещены в эту зону. Укажите зону, созданную на шаге 3.</li> <li>• <b>Профиль Netflow</b> – профиль Netflow, используемый для данного интерфейса. Не обязательный параметр.</li> <li>• <b>Режим</b> - тип присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN, то необходимо использовать статический IP-адрес.</li> <li>• <b>MTU</b> – размер MTU для выбранного интерфейса.</li> </ul> <p>По умолчанию в системе уже создан VPN-интерфейс tunnel2, который рекомендовано использовать для Site-to-Site VPN.</p>
<p><b>Шаг 8.</b> Создать Туннель VPN</p>	<p>VPN-сеть определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и - опционально - маршруты, которые будут переданы клиентам для применения, если клиент поддерживает применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов.</p> <p>Для создания туннеля VPN перейдите в раздел <b>VPN --&gt; Сети VPN</b>, нажмите кнопку <b>Добавить</b> и заполните следующие поля:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> - название сети.</li> <li>• <b>Описание</b> - описание сети.</li> <li>• <b>Диапазон IP-адресов</b>, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.</li> <li>• Укажите <b>DNS-сервера</b>, которые будут переданы клиенту, или поставьте галочку <b>Использовать системные DNS</b>, в этом случае клиенту будут назначены DNS-серверы, которые использует UserGate.</li> <li>• Укажите <b>маршруты</b>, передаваемые клиенту в виде бесклассовой адресации (CIDR)</li> </ul> <p>В UserGate создана сеть <b>Site-to-Site VPN network</b> с настройками по умолчанию. Для использования этой сети в ней необходимо добавить маршруты, передаваемые на сервер-клиент.</p>
<p><b>Шаг 9.</b> Создать серверное правило VPN</p>	<p>Создать серверное правило VPN, используя в нем созданные ранее туннель VPN и профиль VPN. Для создания правила необходимо перейти в раздел <b>VPN --&gt; Серверные правила</b>, нажать кнопку <b>Добавить</b> и заполнить следующие поля:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> - название правила.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Описание</b> - описание правила.</li> <li>• <b>Серверный профиль</b> - серверный профиль, созданный ранее.</li> <li>• <b>Туннель VPN</b> - туннель VPN, созданный ранее.</li> <li>• <b>Профиль авторизации</b> - профиль авторизации, созданный ранее.</li> <li>• <b>Источник</b> - зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону <b>Untrusted</b>.</li> <li>• <b>Интерфейс</b> - созданный ранее интерфейс VPN.</li> <li>• <b>Пользователи</b> - группа учетных записей серверов или отдельные учетные записи серверов, которым разрешено подключаться по VPN.</li> </ul> <p>По умолчанию в UserGate создано серверное правило <b>Site-to-Site VPN rule</b>, в котором используются необходимые настройки для Site-to-Site VPN, а доступ к VPN разрешен членам локальной группе <b>VPN servers</b>.</p> <p>Важно! Для применения различных серверных правил к разным клиентам необходимо использовать параметры <b>Исходная зона</b> и <b>Адрес источника</b>. Параметр <b>Пользователь</b> не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.</p>
--	--

Для настройки сервера, выступающего в роли VPN-клиента, необходимо выполнить следующие шаги:

Наименование	Описание
<p><b>Шаг 1.</b> Создать зону, в которую будут помещен интерфейс, используемый для подключения по VPN</p>	<p>В разделе <b>Сеть --&gt; Зоны</b> создать зону, в которую будут помещены интерфейсы, используемые для подключения по VPN. Эту зону в дальнейшем можно будет использовать в политиках безопасности.</p> <p>Рекомендуется использовать уже существующую по умолчанию зону <b>VPN for Site-to-Site</b>.</p>
<p><b>Шаг 2.</b> Создать разрешающее правило межсетевого экрана для трафика в созданную зону</p>	<p>Создать разрешающее правило межсетевого экрана в разделе <b>Политики сети --&gt; Межсетевой экран</b>.</p> <p>По умолчанию в UserGate создано правило межсетевого экрана <b>VPN for Site-to-Site to Trusted and Untrusted</b>, разрешающее весь трафик между зонами <b>VPN for Site-to-Site, Trusted</b> и <b>Untrusted</b>.</p>
<p><b>Шаг 3.</b> Создать VPN-интерфейс</p>	<p>VPN-интерфейс – это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.</p> <p>В разделе <b>Сеть --&gt; Интерфейсы</b> нажмите кнопку <b>Добавить</b>, и выберите <b>Добавить VPN</b>. Задайте следующие параметры:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> – название интерфейса, должно быть в виде tunnelN, где N – это порядковый номер VPN-интерфейса.</li> <li>• <b>Описание</b> – описание интерфейса.</li> <li>• <b>Зона</b> – зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к серверу UserGate будут так же помещены в эту</li> </ul>

	<p>зону. Укажите зону, созданную на шаге 3.</p> <ul style="list-style-type: none"> <li>• <b>Профиль Netflow</b> – профиль Netflow, используемый для данного интерфейса. Не обязательный параметр.</li> <li>• <b>Режим</b> - тип присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса – Динамический.</li> <li>• <b>MTU</b> – размер MTU для выбранного интерфейса.</li> </ul> <p>По умолчанию в системе уже создан VPN-интерфейс tunnel3, который рекомендовано использовать для клиентского подключения Site-to-Site VPN.</p> <p>Важно! Если при настройке туннельного интерфейса на стороне сервера был выбран уже существующий интерфейс tunnel2 с настройками по умолчанию, то на клиенте при подключении к серверу возникнет конфликт IP-адресов, поскольку на клиенте так же существует аналогичный интерфейс tunnel2 с тем же диапазоном адресов. Для корректной работы диапазоны адресов туннельных интерфейсов не должны пересекаться. Рекомендуется изменить диапазон адресов на клиенте на уникальный.</p>
<p><b>Шаг 4.</b> Создать клиентское правило VPN</p>	<p>Создать клиентское правило VPN, которое будет инициировать подключение к VPN-серверу. Для создания правила необходимо перейти в раздел <b>VPN --&gt; Клиентские правила</b>, нажать кнопку <b>Добавить</b> и заполнить следующие поля:</p> <ul style="list-style-type: none"> <li>• <b>Название</b> - название правила.</li> <li>• <b>Описание</b> - описание правила.</li> <li>• <b>Общий ключ</b> - строка, которая должна совпадать со строкой общего ключа, указанной на сервере.</li> <li>• <b>Безопасность --&gt; Методы шифрования</b> - пары алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, в котором они изображены (сверху вниз). При установлении соединения используется первая пара, которую поддерживают сервер и клиент.</li> <li>• <b>Адрес сервера</b> - IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне <b>Untrusted</b> на сервере UserGate, выполняющего роль VPN-сервера.</li> <li>• <b>Интерфейс</b> - созданный ранее VPN-интерфейс.</li> <li>• <b>Имя пользователя и пароль</b> - имя и пароль пользователя, созданного на шаге 1 при подготовке VPN-сервера.</li> </ul>

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение на сервер, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное правило VPN (на сервере).

## 11 БИБЛИОТЕКИ ЭЛЕМЕНТОВ

Данный большой раздел содержит в себе все записи, адреса-сайтов, IP-адреса, шаблоны и прочие элементы, которые используются при настройке правил UserGate.

Первоначальные данные библиотек поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Некоторые элементы библиотек являются нередактируемыми потому, что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, имеют механизм автоматического обновления. Автоматическое обновление элементов требует наличия специальной лицензии. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование UserGate](#).

### 11.1 Морфология

Морфологический анализ - механизм, который распознает отдельные слова и словосочетания на веб-сайте. Если в тексте содержится достаточное для блокировки количество указанных слов и словосочетаний, то доступ к сайту блокируется.

Морфологический анализ выполняется как при проверке запроса пользователя, так и при получении ответа от веб-сервера и до его передачи пользователю. Получив ответ от веб-сервера, UserGate просматривает текст на странице и подсчитывает его суммарный «вес», исходя из «весов» слов, указанных в морфологических категориях. Если «вес» страницы превышает «вес» морфологической категории, правило срабатывает. При подсчете «веса» страницы учитываются все словоформы (леммы) запрещенных слов. Для поиска словоформ UserGate использует встроенные словари русского, английского, японского, арабского и немецкого языков.

Существует возможность подписки на словари, предоставляемые UserGate. Данные словари нельзя редактировать. Для использования этих словарей необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование UserGate](#).

Наименование	Описание
<b>Соответствие списку запрещенных материалов Министерством Юстиции Российской Федерации</b>	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции Российской Федерации.
<b>Соответствие списку запрещенных материалов республики Казахстан</b>	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции республики Казахстан.
<b>Суицид</b>	Морфологический словарь, содержащий перечень слов и фраз суицидальной направленности.
<b>Терроризм</b>	Морфологический словарь, содержащий перечень слов и фраз террористической направленности.
<b>Нецензурная лексика</b>	Морфологический словарь, содержащий перечень слов и фраз, относящихся к нецензурной лексике.
<b>Азартные игры</b>	Морфологический словарь, содержащий перечень слов и фраз,

	относящихся к азартным играм.
<b>Наркотики</b>	Морфологический словарь, содержащий перечень слов и фраз наркотической направленности.
<b>Соответствие ФЗ-436 (Защита детей)</b>	Морфологический словарь, содержащий перечень слов и фраз тематик, нежелательных для детей.
<b>Порнография</b>	Морфологический словарь, содержащий перечень слов и фраз порнографической направленности.
<b>Бухгалтерия (DLP)</b>	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в бухгалтерии.
<b>Маркетинг (DLP)</b>	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в маркетинге.
<b>Персональные данные (DLP)</b>	Морфологический словарь, содержащий перечень терминов, слов и фраз, встречающихся в персональных данных.
<b>Финансы (DLP)</b>	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в финансах.
<b>Юридический (DLP)</b>	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в юриспруденции.

Для фильтрации по морфологическому содержанию страницы требуется:

Наименование	Описание
<b>Шаг 1.</b> Создать одну или несколько морфологических категорий и указать вес каждой категории	Нажать на кнопку <b>Добавить</b> , задать название новой категории и ее вес.
<b>Шаг 2.</b> Указать список запрещенных фраз с весами	Нажать на кнопку <b>Добавить</b> и указать необходимые слова или фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки.
<b>Шаг 3.</b> Создать правило фильтрации контента, содержащее одну или несколько морфологических категорий	Смотрите раздел <a href="#">Фильтрация контента</a> .

Администратор имеет возможность создать свой словарь и централизованно распространять его на все устройства UserGate имеющиеся в организации. Для создания такой морфологической базы необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать файл с необходимыми фразами	создать файл <b>list.txt</b> со списком слов в следующем формате: <i>!word1 !word2</i> <i>!word3</i> <i>word4 50</i> ... <i>Lastword</i> Вес словаря в таком случае равен 100, вес слова можно указать. По умолчанию он равен 100.
<b>Шаг 2.</b> Создать архив, содержащий этот файл	Поместить файл в архив zip с именем <b>list.zip</b> .
<b>Шаг 3.</b> Создать файл с версией словаря	Создать файл <b>version.txt</b> , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря
<b>Шаг 4.</b> Разместить файлы на веб-сервере	Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.
<b>Шаг 5.</b> Создать морфологическую категорию указать URL для обновления словаря	На каждом UserGate создать морфологическую базу. При создании указать адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять словарь при наличии новой версии.

### Примечание

При создании морфологических словарей не рекомендуется добавлять фразы, содержащие более трех слов, без использования символа «!» перед словами. Необходимо помнить, что при построении морфологической базы каждое из слов будет преобразовано во все существующие формы (склонения, спряжения, множественные числа, времена и т.д.), и результирующее количество фраз будет достаточно большим. При добавлении длинных фраз необходимо использовать модификатор «!» перед словами, модификация которых не нужна, как правило это различные предлоги и союзы. Например, фразу «как уйти из жизни безболезненно» правильно добавить в виде «!как уйти !из !жизни безболезненно». Это сократит количество возможных вариантов фраз, но при этом оставит все фразы с требуемым смыслом.

## 11.2 Сервисы

Раздел сервисы содержит список общеизвестных сервисов, основанных на протоколе TCP/IP, например, таких, как HTTP, HTTPS, FTP и другие. Данные сервисы могут быть использованы при построении правил UserGate. Первоначальный список сервисов поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового сервиса необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать сервис	Нажать на кнопку <b>Добавить</b> , дать сервису название, ввести комментарий.
<b>Шаг 2.</b> Указать протокол и порт	Нажать на кнопку <b>Добавить</b> , выбрать из списка необходимый протокол, указать порты назначения и, опционально, порты источника. Для указания диапазона портов можно использовать - (тире), например, 33333-33355.

## 11.3 IP-адреса

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил UserGate. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать список	На панели Группы нажать на кнопку <b>Добавить</b> , дать название списку IP-адресов.
<b>Шаг 2.</b> Указать адрес обновления списка (не обязательно)	Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе.
<b>Шаг 3.</b> Добавить IP-адреса	На панели Адреса из выбранной группы нажать на кнопку <b>Добавить</b> и ввести адреса. Адреса вводятся в виде IP-адрес или IP-адрес/маска сети, например, 192.168.1.5 192.168.1.0/24.

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать файл с необходимыми IP-адресами	Создать файл <b>list.txt</b> со списком адресов.
<b>Шаг 2.</b> Создать архив,	Поместить файл в архив zip с именем <b>list.zip</b> .

содержащий этот файл	
<b>Шаг 3.</b> Создать файл с версией списка	Создать файл <b>version.txt</b> , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
<b>Шаг 4.</b> Разместить файлы на веб-сервере	Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.
<b>Шаг 5.</b> Создать список IP-адресов и указать URL для обновления	На каждом UserGate создать список IP-адресов. При создании указать адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять список при наличии новой версии.

## 11.4 Useragent браузеров

С помощью фильтрации по Useragent браузеров администратор может запретить или разрешить работу пользователей только с определенным типом браузеров.

Первоначальный список Useragent поставляется вместе с продуктом. Для фильтрации по типу Useragent необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать список Useragent	В панели Категории нажать на кнопку <b>Добавить</b> и задать название нового списка UserAgent и, опционально, описание списка и URL обновления.
<b>Шаг 2.</b> Добавить необходимые Useragent браузеров в новый список	В панели Шаблоны useragent добавить необходимый Useragent. Исчерпывающий список строк Useragent представлен тут: <a href="http://www.useragentstring.com/pages/useragentstring.php">http://www.useragentstring.com/pages/useragentstring.php</a>
<b>Шаг 3.</b> Создать правило фильтрации контента, содержащее один или несколько списков	Смотрите раздел <a href="#">Фильтрация контента</a> .

Администратор имеет возможность создавать свои списки Useragent и централизованно распространять их на все компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать файл с необходимыми Useragent	Создать файл <b>list.txt</b> со списком <b>Useragent</b> .
<b>Шаг 2.</b> Создать архив, содержащий этот файл	Поместить файл в архив zip с именем <b>list.zip</b> .
<b>Шаг 3.</b> Создать файл с	Создать файл <b>version.txt</b> , внутри него указать номер версии списка, например, 3.

версией списка	Необходимо инкрементировать данное значение при каждом обновлении списка.
<b>Шаг 4.</b> Разместить файлы на веб-сервере	Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.
<b>Шаг 5.</b> Создать список Useragent и указать URL для обновления	На каждом UserGate создать список Useragent. При создании указать адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять список при наличии новой версии.

## 11.5 Типы контента

С помощью фильтрации типов контента можно блокировать загрузку файлов определенного типа, например, запретить все файлы типа \*.doc.

Существует возможность подписки на типы контента, предоставляемые разработчиками UserGate. Данные списки типов контента нельзя редактировать, их можно использовать при определении правил фильтрации контента. Для использования этих списков необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование UserGate](#).

Для фильтрации по типу контента необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать список типов контента. Если используется предопределенный список UserGate, перейдите к шагу 3.	В панели <b>Категории</b> нажать на кнопку <b>Добавить</b> , задать название нового списка типа контента и, опционально, описание списка и URL обновления.
<b>Шаг 2.</b> Добавить необходимые типы контента в новый список	Добавить необходимый тип контента в данный список в формате MIME. Различные типы контента и их описание доступны по ссылке <a href="https://www.iana.org/assignments/media-types/media-types.xhtml">https://www.iana.org/assignments/media-types/media-types.xhtml</a> . Например, для блокировки документов типа *.doc необходимо добавить тип контента «application/msword».
<b>Шаг 3.</b> Создать правило фильтрации контента, содержащее один или несколько списков	Смотрите раздел <a href="#">Фильтрация контента</a> .

Администратор имеет возможность создавать свои списки типов контента и централизованно распространять их на все компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать файл с необходимыми типами контента	Создать файл <b>list.txt</b> со списком типов контента.

<b>Шаг 2.</b> Создать архив, содержащий этот файл	Поместить файл в архив zip с именем <b>list.zip</b> .
<b>Шаг 3.</b> Создать файл с версией списка	Создать файл <b>version.txt</b> , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
<b>Шаг 4.</b> Разместить файлы на веб-сервере	Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.
<b>Шаг 5.</b> Создать список типа контента и указать URL для обновления	На каждом UserGate создать список типа контента. При создании указать адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять список при наличии новой версии.

## 11.6 Списки URL

Страница предназначена для задания списков указателей URL, которые могут быть использованы в правилах контентной фильтрации в качестве черных и белых списков.

Компания UserGate предоставляет собственные обновляемые списки. Для использования этих списков необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование UserGate](#).

Наименование	Описание
<b>Список поисковых систем без безопасного поиска</b>	Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля.
<b>Соответствие списку запрещенных URL Министерства Юстиции РФ</b>	Данный список содержит URL, запрещенные Министерством Юстиции Российской Федерации.
<b>Соответствие списку запрещенных URL Республики Казахстан</b>	Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан.
<b>Список образовательных учреждений</b>	Список доменных имен образовательных учреждений РФ.
<b>Список фишинговых сайтов</b>	Данный список содержит URL фишинговых сайтов.
<b>Соответствие реестру запрещенных сайтов Роскомнадзора (URL)</b>	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте <a href="http://eais.rkn.gov.ru">http://eais.rkn.gov.ru</a> .
<b>Соответствие реестру запрещенных сайтов</b>	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте

Роскомнадзора (домены)	http://eais.rkn.gov.ru.
------------------------	-------------------------

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать список URL	В панели Списки URL нажать на кнопку *Добавить*, задать название нового списка.
<b>Шаг 2.</b> Добавить необходимые записи в новый список	Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «\$» и «*»:  «*» - любое количество любых символов  «^» - начало строки  «\$» - конец строки  Символы «?» и «#» не могут быть использованы.
<b>Шаг 3.</b> Создать правило фильтрации контента, содержащее один или несколько списков	Смотрите раздел <a href="#">Фильтрация контента</a> .

Если URL-запись начинается с «http://», «https://», «ftp://» или содержит один или более символов «/», то это считается URL и применяется только для HTTP(S) фильтрации, к DNS-фильтрации такая запись не применяется. В противном случае строка рассматривается как имя домена и применяется для DNS-фильтрации и HTTP(S)-фильтрации.

Если вы хотите заблокировать точный адрес, используйте символы «^» и «\$»:

`^http://domain.com/exacturl$`

Для блокирования точного URL всех дочерних папок используйте символ «^»:

`^http://domain.com/exacturl/`

Для блокирования домена со всеми возможными URL используйте запись такого вида:

`domain.com`

Пример интерпретации URL-записей:

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Блокируется весь домен и домены 3 уровня, например:  sport.yahoo.com  mail.yahoo.com	блокируется весь домен и все URL этого домена и домены 3 уровня, например:  <a href="http://sport.yahoo.com">http://sport.yahoo.com</a>  <a href="http://mail.yahoo.com">http://mail.yahoo.com</a>  <a href="https://mail.yahoo.com">https://mail.yahoo.com</a>

	а также: qweryyahoo.com	<a href="http://sport.yahoo.com/123">http://sport.yahoo.com/123</a>
^mail.yahoo.com\$	Заблокирован только mail.yahoo.com	заблокированы только <a href="http://mail.yahoo.com">http://mail.yahoo.com</a> <a href="https://mail.yahoo.com">https://mail.yahoo.com</a>
^mail.yahoo.com/\$	Ничего не заблокировано	Ничего не заблокировано, так как последний символ слэш определяет URL, но не указаны «https» или «http»
^http://finance.yahoo.com/personal-finance/\$	Ничего не заблокировано	заблокирован только <a href="http://finance.yahoo.com/personal-finance/">http://finance.yahoo.com/personal-finance/</a>
^yahoo.com/12345/	Ничего не заблокировано	заблокированы <a href="http://yahoo.com/12345/whatever/">http://yahoo.com/12345/whatever/</a> <a href="https://yahoo.com/12345/whatever/">https://yahoo.com/12345/whatever/</a>

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все компьютеры с установленным UserGate. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать файл с необходимым списком URL	Создать текстовый файл <b>list.txt</b> со списком URL в следующем формате: <i>www.site1.com/url1</i> <i>www.site2.com/url2</i> ... <i>www.siteend.com/urlN</i>
<b>Шаг 2.</b> Создать архив, содержащий этот файл	Поместить файл в архив zip с именем <b>list.zip</b> .
<b>Шаг 3.</b> Создать файл с версией списка	Создать файл <b>version.txt</b> , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
<b>Шаг 4.</b> Разместить файлы на веб-сервере	Разместить у себя на сайте <b>list.zip</b> и <b>version.txt</b> , чтобы они были доступны для скачивания.
<b>Шаг 5.</b> Создать список типа контента и указать URL для обновления	На каждом UserGate создать список URL. При создании указать адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять список при наличии новой версии.

## 11.7 Календари

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах UserGate. Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать календарь	В панели Группы нажать на кнопку <b>Добавить</b> , указать название календаря и его описание.
<b>Шаг 2.</b> Добавить временные интервалы в календарь	В панели Элементы нажать на кнопку <b>Добавить</b> и добавить интервал. Дать название интервалу и указать время.

## 11.8 Полосы пропускания

Элемент библиотеки **Полоса пропускания** определяет скорость передачи данных, которую возможно в дальнейшем использовать в правилах управления полосой пропускания. Более подробно о правилах управления полосой пропускания смотрите в главе [Пропускная способность](#).

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления новой полосы пропускания необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать полосу пропускания	Нажать на кнопку <b>Добавить</b> , дать название, описание.
<b>Шаг 2.</b> Указать скорость	Указать скорость в Кбит/сек.
<b>Шаг 3.</b> Указать значение DSCP для QoS	Необязательный параметр. Если установлен, то будет прописываться в каждый IP пакет. Диапазон от 0 до 63.

## 11.9 Профили АСУ ТП

Профиль АСУ ТП - это набор элементов, каждый из которых состоит из определенной команды АСУ ТП и адреса. Профиль АСУ ТП используется в правилах АСУ ТП. Более подробно о фильтрации трафика АСУ ТП читайте в разделе [Правила АСУ ТП](#).

## 11.10 Шаблоны страниц

С помощью шаблонов страниц администратор может управлять видом страницы блокировки и страницы авторизации Captive-портала. Администратор может использовать разные шаблоны для разных правил фильтрации контента и правил Captive-портала.

UserGate поставляется с тремя типами шаблонов - шаблоны для Captive-портала, шаблоны контроля сессии пользователя и шаблоны для страницы блокировки. Они могут использоваться как образцы для создания пользовательских шаблонов, например, в фирменном стиле компании или на необходимом языке.

Наименование	Описание
Шаблоны <b>Blockpage (EN)</b> и <b>Blockpage (RU)</b>	Стандартные шаблоны блокировки на английском и русском языках.
Шаблоны <b>Captive portal user auth (EN)</b> и <b>Captive portal user auth (RU)</b>	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль). При успешной авторизации пользователь получает доступ в интернет.
Шаблоны <b>Captive portal user auth + policy (EN)</b> и <b>Captive portal user auth + policy (RU)</b>	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль), правила пользования сетью (соглашение об использовании), а также требует принятия пользователем правил политики доступа. При успешной авторизации пользователь получает доступ в интернет.
Шаблоны <b>Captive portal: email auth (EN)</b> и <b>Captive portal: email auth (RU)</b>	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя письмом по e-mail. Для корректной работы данных шаблонов необходимо настроить раздел <b>Оповещения</b> в Captive-профиле.
Шаблон <b>Captive portal: SMS auth (EN)</b> и <b>Captive portal: SMS auth (RU)</b>	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя с помощью SMS. Для корректной работы данных шаблонов необходимо настроить раздел <b>Оповещения</b> в Captive-профиле.
Шаблон <b>Captive portal policy (EN)</b> и <b>Captive portal policy (RU)</b>	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. При согласии с политикой доступа пользователь получает доступ в интернет. Для работы данного шаблона требуется установить метод <b>Принять политику</b> в качестве метода аутентификации в Captive-профиле.
Шаблоны <b>Captive portal user session (EN)</b> и <b>Captive portal user session (RU)</b>	Шаблоны на английском и русском языках, с помощью которых пользователь может завершить свою авторизованную сессию, перейдя на страницу <a href="http://logout.captive">http://logout.captive</a> или <a href="http://USERGATE_IP/cps">http://USERGATE_IP/cps</a> .
Шаблоны <b>Content warning (EN)</b> и <b>Content warning (RU)</b>	Шаблоны на английском и русском языках, содержащие страницу предупреждения, отображаемую при срабатывании правила контентной фильтрации с действием <b>Предупредить</b> .

Шаблоны <b>FTP client (EN)</b> и <b>FTP client (RU)</b>	Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP.
Шаблоны <b>web portal page (EN)</b> и <b>(RU)</b>	Шаблоны на английском и русском языках для отображения страницы веб-портала.
Шаблоны <b>web portal login page for RDP (EN)</b> и <b>(RU)</b>	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал.
Шаблоны <b>web portal login page for SSH (EN)</b> и <b>(RU)</b>	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал.
Шаблоны <b>TOTP INIT PAGE (EN)</b> и <b>TOTP INIT PAGE (RU)</b>	Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей.

Для создания собственного шаблона необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Экспортировать существующий шаблон, поставляемый по умолчанию	Выбрать один из существующих шаблонов, нажать на кнопку <b>Экспорт</b> и сохранить шаблон в файле.
<b>Шаг 2.</b> Изменить экспортированный шаблон	Используя редактор, изменить содержание шаблона. Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут испортить внутреннюю структуру шаблона. Используйте простые редакторы текста.
<b>Шаг 3.</b> Создать новый шаблон	Нажать на кнопку <b>Добавить</b> , выбрать соответствующий тип шаблона, задать название шаблону и сохранить его.
<b>Шаг 4.</b> Импортировать измененный на шаге 2 шаблон	Выделить вновь созданный шаблон, нажать на кнопку <b>Импорт</b> и выбрать файл с измененным шаблоном.

## 11.11 Категории URL

Элемент библиотеки **Категория URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. Например, администратор может создать группу категорий «Бизнес категории» и поместить в нее необходимые категории.

Для использования категорий UserGate URL filtering требуется наличие специальной лицензии.

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы.

Наименование	Описание
--------------	----------

<b>Threats</b>	Набор категорий, рекомендованных для блокировки в целях обеспечения безопасности сети.
<b>Parental Control</b>	Набор категорий, рекомендованных для блокировки в целях защиты детей от нежелательного контента.
<b>Productivity</b>	Набор категорий, рекомендованных для блокировки в целях повышения эффективности работы сотрудников.
<b>Safe categories</b>	Набор категорий, считаемых безопасными для посещения. Рекомендуется отключать морфологическую проверку, перехват HTTPS-трафика для данной группы категорий в целях уменьшения количества ложных срабатываний.
<b>Recommended for morphology checking</b>	Набор категорий, рекомендованных для проверки с помощью морфологического анализа. Из этого набора исключены такие категории, как «Новости», «Финансы», «Правительство», «Информационная безопасность», «Детские сайты» и ряд других в целях уменьшения количества ложных срабатываний. Этот же набор категорий рекомендуется использовать для перехвата трафика HTTPS.
<b>Recommended for virus check</b>	Набор категорий, рекомендованных для антивирусной проверки.

Для добавления новой группы категорий необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать группу категорий	Нажать на кнопку <b>Добавить</b> , дать название группе.
<b>Шаг 2.</b> Добавить категории	Нажать на кнопку <b>Добавить</b> и выбрать необходимые категории из списка.

## 11.12 Измененные категории URL

Элемент библиотеки **Измененные категория URL** позволяет администратору назначить определенным сайтам категории, отличные от категорий, назначенных техническими специалистами UserGate. Такая потребность может возникнуть в случае некорректного категорирования сайтов или в случае, если требуемый сайт не имеет назначенной ему категории. Для переопределения категории сайта необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Проверить первоначальную категорию сайта	В разделе <b>Библиотеки --&gt; Измененные категории URL</b> ввести требуемый адрес сайта в строку проверки и нажать на кнопку <b>Проверить категорию</b> .
<b>Шаг 2.</b> Назначить новую категорию	Если полученная категория не совпадает с требуемой, то необходимо нажать на кнопку <b>Добавить</b> и назначить до двух новых категорий.

После успешного изменения категории сайт будет отображаться в списке сайтов с измененными категориями. Для него также будет указаны дата изменения категории, администратор, выполнивший данное изменение, его оригинальные и новые категории.

При последующей проверке категорий для данного сайта в качестве категорий будут возвращены только новые категории и специальная категория, в которую включаются все сайты с измененными категориями - **Переопределенные пользователем категории**.

Администратор может экспортировать списки сайтов с измененными категориями или импортировать любые списки сайтов и назначить им требуемые категории.

## 11.13 Приложения

Элемент библиотеки **Приложения** позволяет создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика. Например, администратор может создать группу приложений «Бизнес приложения» и поместить в нее необходимые приложения.

Для добавления новой группы приложений необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать группу приложений	Нажать на кнопку <b>Добавить</b> , дать название группе.
<b>Шаг 2.</b> Добавить приложения	Нажать на кнопку <b>Добавить</b> и выбрать необходимые приложения из списка.

## 11.14 Почтовые адреса

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать группу почтовых адресов	Нажать на кнопку <b>Добавить</b> , дать название группе.
<b>Шаг 2.</b> Добавить почтовые адреса в группу	Нажать на кнопку <b>Добавить</b> и добавить необходимые почтовые адреса.

## 11.15 Номера телефонов

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Создать группу телефонных номеров	Нажать на кнопку <b>Добавить</b> , дать название группе.
<b>Шаг 2.</b> Добавить номера телефонов в группу	Нажать на кнопку <b>Добавить</b> и добавить необходимые номера.

## 11.16 Профили COB

Профиль COB - это набор сигнатур, релевантных для защиты определенных сервисов. Администратор может создать необходимое количество профилей COB для защиты различных сервисов. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты сервиса. Например, для защиты сервиса, работающего по протоколу TCP, не стоит добавлять сигнатуры, разработанные для протокола UDP. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора. Более подробно о создании и использовании профилей COB смотрите в разделе [Система обнаружения и предотвращения вторжений](#).

## 11.17 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 **Оповещения -- > Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
<b>Название</b>	Название профиля.
<b>Описание</b>	Описание профиля.
<b>Хост</b>	IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
<b>Порт</b>	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 .
<b>Безопасность</b>	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
<b>Авторизация</b>	Включает авторизацию при подключении к SMTP-серверу.
<b>Логин</b>	Имя учетной записи для подключения к SMTP-серверу.

<b>Пароль</b>	Пароль учетной записи для подключения к SMTP-серверу.
---------------	---

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

Наименование	Описание
<b>Название</b>	Название профиля.
<b>Описание</b>	Описание профиля.
<b>Хост</b>	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
<b>Порт</b>	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL – 3550.
<b>SSL</b>	Использовать или нет шифрацию с помощью SSL.
<b>Авторизация</b>	Включает авторизацию при подключении к SMPP-серверу.
<b>Логин</b>	Имя учетной записи для подключения к SMPP-серверу.
<b>Пароль</b>	Пароль учетной записи для подключения к SMPP-серверу.
<b>Правила трансляции номеров</b>	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.

## 11.18 Профили Netflow

Профиль Netflow позволяет указать параметры необходимые для отсылки информации на коллектор Netflow. Для создания профиля Netflow необходимо нажать на кнопку **Добавить** в разделе **Библиотеки --> Профили Netflow** и указать необходимые параметры:

Наименование	Описание
<b>Название</b>	Название профиля Netflow
<b>Описание</b>	Описание профиля Netflow
<b>IP-адрес Netflow коллектора</b>	IP-адрес сервера, куда сенсор будет отправлять статистику.

<b>Порт Netflow коллектора</b>	UDP порт, на котором коллектор будет принимать статистику.
<b>Версия протокола</b>	Версия протокола Netflow, которую следует использовать. Версия протокола должна совпадать на сенсоре и на коллекторе.
<b>Таймаут активного потока (сек)</b>	При длительных потоках, например, передача большого файла через сеть, время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока. Значение по умолчанию – 1800 секунд.
<b>Таймаут неактивного потока (сек.)</b>	Время, резервируемое на завершение неактивного потока. Значение по умолчанию – 15 секунд.
<b>Количество потоков</b>	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. Ограничение необходимо для защиты от DoS-атак. После достижения данного количества потоков, все последующие не будут учитываться. Значение по умолчанию - 2000000, установите 0 для снятия ограничения.
<b>Отправлять информацию NAT</b>	Отправлять информацию о NAT преобразованиях в статистику Netflow.
<b>Частота отправки шаблона (пакетов)</b>	Количество пакетов, после которых шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию – 20 пакетов.
<b>Период отправки старого шаблона (сек.)</b>	Время, через которое старый шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию – 1800 секунд.

## 12 ДАШБОРД

Данный раздел позволяет посмотреть текущее состояние сервера, его загрузку, количество пользователей, объемы трафика, проходящего через сервер, работу систем фильтрации, статус лицензии и так далее. Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами NOC (Network Operation Center) и SOC (Security Operation Center).

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
<b>Название</b>	Название виджета, которое будет отображаться в Дашборд.
<b>Описание</b>	Опциональное описание виджета.
<b>Количество записей</b>	Максимальное количество записей для отображения.
<b>Группировать по</b>	Поле данных, по которому будут сгруппированы данные в виджете.
<b>Диаграмма</b>	Выбор типа представления данных. Доступны значения: <ul style="list-style-type: none"><li>• Число</li><li>• Круговая диаграмма</li><li>• Вертикальная гистограмма</li><li>• Горизонтальная гистограмма</li><li>• Таблица</li><li>• График</li><li>• Карта мира</li></ul>
<b>Запрос фильтра</b>	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а так же примеры их использования можно посмотреть в разделе документации <a href="#">Поиск и фильтрация данных</a> .

## 13 ДИАГНОСТИКА И МОНИТОРИНГ

### 13.1 Маршруты

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

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

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

### 13.2 VPN

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

- **Пользователь** - имя пользователя, под которым произошла авторизация соединения.
- **Тип** - клиент или сервер.
- **Продолжительность** - продолжительность установленного соединения.
- **Гео IP источника** - страна по Geo IP, откуда установлено соединение.
- **Шифрование** - тип шифрования.
- **Скорость передачи** - скорость передачи информации на момент отображения данной страницы.
- **Скорость приема** - скорость приема информации на момент отображения данной страницы.
- **Передано байт** - объем переданной информации.
- **Принято байт** - объем принятой информации.
- **Передано пакетов** - количество переданных пакетов с начала VPN-сессии.
- **Принято пакетов** - количество принятых пакетов с начала VPN-сессии.

### 13.3 Веб-портал

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

- **Пользователь** - имя пользователя, под которым произошла авторизация соединения.
- **Начало сессии** - время, когда пользователь подключился к сервису.
- **IP источника** - IP-адрес пользователя.
- **Useragent** - useragent пользовательского браузера.

## 13.4 Захват пакетов

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

Раздел состоит из трех частей:

- **Фильтры** - здесь определяются условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол Ethernet, протокол IPv4. Список протоколов IPv4 можно посмотреть по ссылке <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>.
- **Правила** - в правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.
- **Файлы** - сюда помещаются файлы с записанным трафиком. Их можно скачать для анализа или удалить.

Чтобы записать трафик, необходимо выполнить следующие шаги:

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

## 13.5 Запросы в белый список

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

Наименование	Описание
<b>Добавить в белый список</b>	Добавить данный URL в белый список. Администратору будет предложено изменить URL и выбрать белый список, в который необходимо добавить данный ресурс.
<b>Удалить</b>	Удалить данный запрос из списка запросов.

<b>Отклонить URL</b>	Добавить запрошенный URL в список отклоненных запросов. При последующих блокировках данного URL страница блокировки не будет содержать кнопки <b>Добавить в белый список</b> . Список отклоненных доменов и URL отображается в <b>Окне отклоненных запросов</b> .
<b>Отклонить домен</b>	Добавить домен запрошенного URL в список отклоненных запросов. При последующих блокировках любого URL данного домена страница блокировки не будет содержать кнопки <b>Добавить в белый список</b> . Список отклоненных доменов и URL отображается в <b>Окне отклоненных запросов</b> .

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

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

Для того, чтобы сменить категории локально, необходимо нажать на кнопку **Изменить категорию** и назначить до двух новых категорий. Посмотреть все сайты с измененными категориями можно в разделе **Библиотеки --> Измененные категории URL**. При последующей проверке категорий для данного сайта в качестве категорий будут возвращены только новые категории и специальная категория, в которую включаются все сайты с измененными категориями - **Переопределенные пользователем категории**. Более подробно об изменении категорий для определенных сайтов описано в разделе руководства [Запросы в белый список](#).

## 13.6 Трассировка правил

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

Наименование	Описание
<b>Шаг 1.</b> Создать необходимый фильтр	<p>Нажать на кнопку <b>Настроить</b> в разделе <b>Диагностика и мониторинг --&gt; Трассировка правил</b> и указать параметры фильтра:</p> <ul style="list-style-type: none"> <li>• <b>Строка</b> - строка в запросе пользователя, например, имя домена, URL, правила контентной фильтрации</li> <li>• <b>Пользователь</b> - пользователь, обработку запросов которого необходимо продиагностировать</li> <li>• <b>IP-адрес источника</b> - IP-адрес с которого пользователь осуществляет запрос</li> </ul> <p>Фильтр необходим для ограничения вывода диагностической информации. Если его не задать, то могут быть так же отображены результаты обработки запросов других пользователей.</p>
<b>Шаг 2.</b> Запустить трассировку	Нажать на кнопку <b>Начать</b> .

<b>Шаг 3.</b> Открыть проблемный сайт	Попросить пользователя открыть проблемный сайт и наблюдать, какие правила срабатывают при открытии сайта. Будут указаны все правила, которые выполняются во время обработки пользовательского запроса.
---------------------------------------	--

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

## 13.7 Ping

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

Наименование	Описание
<b>Ping host</b>	Хост, который необходимо проверить.
<b>TTL</b>	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту.
<b>Интерфейс</b>	С какого сетевого интерфейса выполнять ping.
<b>Счетчик</b>	Количество повторов.
<b>Показывать timestamp</b>	Добавляет timestamp в вывод команды.
<b>Не резолвить имена</b>	Оперировать IP-адресами, не преобразовывая их в доменные имена.

## 13.8 Traceroute

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

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

## 13.9 Запрос DNS

Используя запрос DNS администратор может проверить работу DNS-серверов.

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

## 13.10 Оповещения

### 13.10.1 Правила оповещений

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

Наименование	Описание
<b>Шаг 1.</b> Создать один или несколько профилей оповещения	Смотрите раздел <a href="#">Профили оповещений</a> .
<b>Шаг 2.</b> Создать группы получателей оповещений	Смотрите разделы <a href="#">Почтовые адреса</a> и <a href="#">Номера телефонов</a> .
<b>Шаг 3.</b> Создать правило оповещения	В разделе <b>Библиотеки</b> --> <b>Правила оповещений</b> добавить правило.

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включает или отключает данное правило.
<b>Название</b>	Название правила.
<b>Описание</b>	Описание правила.
<b>Профиль оповещения</b>	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для

	указания адресатов в виде e-mail-адресов.
<b>От</b>	От кого будет приходить оповещение.
<b>Тема</b>	Тема оповещения.
<b>Таймаут перед повторной отправкой, секунд</b>	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
<b>События</b>	Укажите события, для которых необходимо получать оповещения.
<b>Телефоны</b>	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.
<b>Emails</b>	Для SMTP-профиля. Укажите группы адресов e-mail, на которые будут отправляться почтовые оповещения.

### 13.10.2 SNMP

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается управление как с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps). Это позволяет наблюдать за критическими параметрами UserGate с помощью программного обеспечения SMNP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP необходимо создать правила SNMP. Для создания правила SNMP необходимо выбрать меню Диагностика и мониторинг и в разделе SNMP нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
<b>Название правила</b>	Название правила.
<b>IP-адрес сервера для трапов</b>	IP-адрес сервера для трапов и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
<b>Комьюнити</b>	SNMP community - строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
<b>Контекст</b>	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры.
<b>Версия</b>	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
<b>Разрешить SNMP-запросы</b>	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.

<b>Разрешить SNMP-трапы</b>	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
<b>Пользователь</b>	Только для SNMP v3. Имя пользователя для авторизации SNMP-менеджера.
<b>Тип аутентификации</b>	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: <ul style="list-style-type: none"> <li>• Без аутентификации, без шифрования (noAuthNoPriv).</li> <li>• С аутентификацией, без шифрования (authNoPriv).</li> <li>• С аутентификацией, с шифрованием (authPriv).</li> </ul> Наиболее безопасным считается режим работы authPriv.
<b>Алгоритм аутентификации</b>	Алгоритм, используемый для аутентификации.
<b>Пароль аутентификации</b>	Пароль, используемый для аутентификации.
<b>Алгоритм шифрования</b>	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
<b>Пароль шифрования</b>	Пароль, используемый для шифрования.
<b>События</b>	Параметры, значения которых будут доступны для считывания SNMP-менеджером. Если отсылка трапов была разрешена, то при достижении критичного значения параметра на сервер будет отправлен трап.



### Примечание

Настройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate.

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

Кнопка **Скачать MIB** позволяет скачать mib-файлы с параметрами мониторинга UserGate для последующего использования их в SNMP-менеджере. UserGate выделен уникальный идентификатор **SNMP PEN** (Private Enterprise Number) **45741**.

## 14 ЖУРНАЛЫ И ОТЧЕТЫ

### 14.1 Журналы

Usergate журналирует все события, которые происходят во время его работы, и записывает их в следующие журналы:

- Журнал событий – события, связанные с изменением настроек сервера UserGate, авторизация пользователей, администраторов, обновлений различных списков и т.п.
- Журнал веб-доступа – подробный журнал всех веб-запросов, обработанных UserGate.
- Журнал трафика – подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing. Для регистрации данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing.
- Журнал COB – события, регистрируемые системой обнаружения и предотвращения событий.
- История поиска – поисковые запросы пользователей в популярных поисковых системах.

#### 14.1.1 Журнал событий

Журнал событий отображает события, связанные с изменением настроек сервера UserGate, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал или VPN, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **\*Показать\*** выведет окно с подробным описанием события.

#### 14.1.2 Журнал веб-доступа

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL, Веб-безопасности, Captive-портала в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действия.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.

- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP назначения.
- Порт назначения.
- Категории.
- Протокол (HTTP).
- Метод (HTTP).
- Код ответа (HTTP).
- Тип контента (если присутствует).
- Байт передано/получено.
- Пакетов отправлено.
- Реферер (при наличии).
- Операционная система.
- Браузер.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

### 14.1.3 Журнал трафика

Журнал трафика отображает события срабатывания правил межсетевого экрана и правил NAT, в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Протокол.
- Зона источника.
- Адрес источника.
- Порт источника.
- Зона назначения.
- IP-назначения.
- Порт назначения.
- NAT IP-источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

#### 14.1.4 Журнал COB

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры COB, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Действие.
- Сигнатура.
- Класс - класс сигнатуры.
- CVE - номер уязвимости по базе CVE.
- Bugtrack - номер уязвимости по базе Bugtrack.
- Nessus - номер уязвимости по базе Nessus.
- Протокол.
- IP источника.
- Порт источника.
- IP назначения.
- Порт назначения.
- Подробности срабатывания сигнатуры.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

#### 14.1.5 История поиска

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

### 14.1.6 Поиск и фильтрация данных

Количество записей, регистрируемых в журналах, как правило, очень велико, и не все поля доступны в базовом режиме просмотра. UserGate предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
<b>AND</b> или <b>and</b>	Логическое И, требует выполнения всех условий, заданных в запросе.
<b>OR</b> или <b>or</b>	Логическое ИЛИ, достаточно выполнения одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
<b>=</b>	Равно. Требуется полного совпадения значения поля указанному значению, например, <i>ip=172.16.31.1</i> будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
<b>!=</b>	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, <i>ip!=172.16.31</i>

	будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<b>&lt;=</b>	Меньше либо равно. Значение поля должно быть меньше либо равно указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>date &lt;= '2019-03-28T20:59:59' AND statusCode=303</i>
<b>&gt;=</b>	Больше либо равно. Значение поля должно быть больше либо равно указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>date &gt;= "2019-03-13T21:00:00" AND statusCode=200</i>
<b>&lt;</b>	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>date &lt; '2019-03-28T20:59:59' AND statusCode=404</i>
<b>&gt;</b>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>(statusCode&gt;200 AND statusCode &lt;300) OR (statusCode=404)</i>
<b>IN</b>	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, например, <i>category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')</i>
<b>~</b>	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, <i>browser ~ "Mozilla/5.0"</i> Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
<b>!~</b>	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, <i>browser !~ "Mozilla/5.0"</i> Данный оператор может быть применен только к полям, в которых хранятся строковые данные.

При составлении расширенного запроса UserGate показывает возможные варианты названия полей, применимых к ним операторов и возможных значений, облегчая оператору системы формирование сложных запросов. Список полей и их возможных значений может отличаться для каждого из журналов.

При переключении режима поиска с основного на расширенный UserGate автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

## 14.1.7 Экспорт журналов

Функция экспортирования журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал СОВ.
- Журнал трафика.
- Журнал АСУ ТП.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
<b>Название правила</b>	Название правила экспорта журналов.
<b>Описание</b>	Оptionальное поле для описания правила.
<b>Журналы для экспорта</b>	<p>Выбор файлов журналов, которые необходимо экспортировать:</p> <ul style="list-style-type: none"><li>• Журнал событий.</li><li>• Журнал веб-доступа.</li><li>• Журнал СОВ.</li><li>• Журнал трафика.</li><li>• Журнал АСУ ТП.</li></ul> <p>Для каждого из журналов возможно указать синтаксис выгрузки:</p> <ul style="list-style-type: none"><li>• CEF – Common Event Format (ArcSight).</li><li>• JSON – JSON format.</li><li>• @CEE: JSON - CEE Log Syntax (CLS) Encoding JSON.</li></ul> <p>Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов.</p>
<b>Тип сервера</b>	SSH (SFTP), FTP, Syslog.
<b>Адрес сервера</b>	IP-адрес или доменное имя сервера.
<b>Транспорт</b>	Только для типа серверов Syslog - TCP или UDP.
<b>Порт</b>	Порт сервера, на который следует отправлять данные.

<b>Протокол</b>	Только для типа серверов Syslog – RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
<b>Критичность</b>	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: 1 - Alert: action must be taken immediately. 2 - Critical: critical conditions. 3 - Error: error conditions. 4 - Warning: warning conditions. 5 - Notice: normal but significant condition. 6 - Informational: informational messages.
<b>Facility</b>	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: 1 - User-level messages. 3 - System daemons. 10 - Security/authorization messages. 13 - Log audit. 14 - Log alert. 16 - Local use 0 (local0). 17 - Local use 1 (local1). 18 - Local use 2 (local2). 19 - Local use 3 (local3). 20 - Local use 4 (local4). 21 - Local use 5 (local5). 22 - Local use 6 (local6). 23 - Local use 7 (local7).
<b>Имя хоста</b>	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
<b>App-Name</b>	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
<b>Логин</b>	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
<b>Пароль</b>	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу

	отправки Syslog.
<b>Путь на сервере</b>	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.
<b>Расписание</b>	<p>Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты:</p> <ul style="list-style-type: none"> <li>• Ежедневно.</li> <li>• Еженедельно.</li> <li>• Ежемесячно</li> <li>• Каждые ... часов.</li> <li>• Каждые ... минут.</li> <li>• Задать вручную.</li> </ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"> <li>• Звездочка (*) - обозначает весь диапазон (от первого до последнего).</li> <li>• Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.</li> <li>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li> <li>• Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "* / 2" в поле "часы" будет означать "каждые два часа".</li> </ul>
<b>Управление журналами</b>	<p>Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp.</p> <p>При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.</p> <p>Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день.</p>

## 14.2 Отчеты

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел отчеты состоит из трех подразделов - шаблоны, правила и созданные отчеты. Что бы создать отчет необходимо выполнить следующие действия:

Наименование	Описание
<b>Шаг 1.</b> Создать правило	Создать правило создания отчета, в котором указать необходимые параметры

создания отчета	создания отчета.
<b>Шаг 2.</b> Запустить отчет	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
<b>Шаг 3.</b> Получить отчет	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе <b>Созданные отчеты</b> .

### **Примечание**

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.

## 14.2.1 Шаблоны отчетов

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией разработчиком UserGate.

Список возможных шаблонов отчетов, сгруппированных по категориям:

- События - группа шаблонов по событиям, регистрируемым в журнале событий.
- COB - группа шаблонов по событиям, регистрируемым в журнале COB.
- Сетевая активность - группа шаблонов по событиям, регистрируемым в журнале трафика.
- Трафик - группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- Веб-активность - группа шаблонов по событиям, регистрируемым в журнале веб-доступа.
- Веб-портал - группа шаблонов по событиям, относящимся к работе веб-портала.
- Captive-портал - группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

## 14.2.2 Правила отчетов

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
<b>Вкл</b>	Включение/отключения отчета.
<b>Название</b>	Название правила.
<b>Описание</b>	Опциональное поле для описания правила.

<b>Язык отчета</b>	Выбор языка, который будет использован в отчете.
<b>Диапазон</b>	Диапазон времени, за который необходимо подготовить отчет.
<b>Формат отчета</b>	<p>Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет.</p> <p>Важно! Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Не используйте формат отчета PDF для пользовательских шаблонов. Для шаблонов <b>Подробный список всех посещенных URL</b> и <b>Подробный список всех посещенных сайтов</b> автоматически используется формат CSV, независимо от выбранного формата.</p>
<b>Количество записей</b>	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
<b>Количество в группировке (если применимо)</b>	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям - для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
<b>Пользователи</b>	Задаёт пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
<b>Шаблоны</b>	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.
<b>Расписание</b>	<p>Выбор расписания для создания отчетов. Возможны варианты:</p> <ul style="list-style-type: none"> <li>• Ежедневно.</li> <li>• Еженедельно.</li> <li>• Ежемесячно.</li> <li>• Каждые ... часов.</li> <li>• Каждые ... минут.</li> <li>• Задать вручную.</li> </ul> <p>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:</p> <ul style="list-style-type: none"> <li>• Звездочка (*) - обозначает весь диапазон (от первого до последнего).</li> <li>• Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7</li> <li>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23"</li> </ul> <p>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "* / 2" в поле "часы" будет означать "каждые два часа".</p>
<b>Доставка</b>	Возможность задать опциональную отправку созданного отчета получателям по протоколу

---

SMTP. Необходимо задать:

- Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе **Оповещения**.
  - От - имя отправителя письма.
  - Тема письма - тема письма (subject).
  - Тело письма - содержимое письма.
  - Получатели - список получателей письма. Получатели должны быть добавлены в списки библиотеки **Почтовые адреса**.
- 

---

### **Примечание**

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

---

---

### **Примечание**

Для того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать на кнопку **Запустить сейчас**. Готовый отчет после создания будет доступен в разделе **Созданные отчеты**.

---

## 14.2.3 Созданные отчеты

В разделе **Созданные отчеты** хранятся все полученные отчеты. Отчеты создаются в формате pdf или csv. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, которое было использовано для создания данного отчета, время создания отчета и размер отчета.

Для скачивания отчета необходимо кликнуть на файл с созданным отчетом, для удаления - **Удалить**.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**. Значение по умолчанию - 60 дней.

## 15 ГОСТЕВОЙ ПОРТАЛ

Данный раздел предназначен для управления временными (гостевыми) учетными записями пользователей. Подробное описание данного раздела описано в главе [Управление гостевыми пользователями](#).

## 16 ПОМОЩЬ

Раздел предоставляет ссылки на полезные ресурсы портала технической поддержки UserGate:

Наименование	Описание
<b>Помощь</b>	Ссылка на актуальную версию руководства администратора.
<b>Обучающее видео</b>	Ссылка на список видеороликов, объясняющих настройку различных служб UserGate.
<b>Поддержка</b>	Ссылка на портал службы технической поддержки UserGate на сайте компании <a href="https://www.usergate.com/ru/support">https://www.usergate.com/ru/support</a> содержит дополнительную информацию по настройке UserGate. Кроме этого, здесь же вы можете оставить заявку на решение вашей проблемы.

## 17 ADMIN

Данный раздел позволяет зарегистрированному администратору сменить свой пароль, изменить некоторые настройки профиля и выйти из системы.

Наименование	Описание
<b>Сменить пароль</b>	Для смены пароля необходимо указать свой текущий пароль и два раза указать новый пароль.
<b>Предпочтения</b>	<ul style="list-style-type: none"><li>• Количество элементов на странице - устанавливает количество строк, отображаемых в одном диалоговом окне, например, список правил межсетевого экрана.</li><li>• Популярные фильтры - изменение названия или удаление фильтров различных журналов, созданных данным пользователем.</li></ul>
<b>Выход</b>	Завершение сеанса работы в веб-консоли устройства.

## 18 ПРИЛОЖЕНИЕ 1. УСТАНОВКА СЕРТИФИКАТА ЛОКАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика, как это описано в главе **Управление сертификатами**, и следуйте инструкциям по установке сертификата ниже в этом разделе.

### 18.1 Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

Откройте папку, куда вы скачали pem-сертификат, переименуйте его в user.der и дважды нажмите на него:

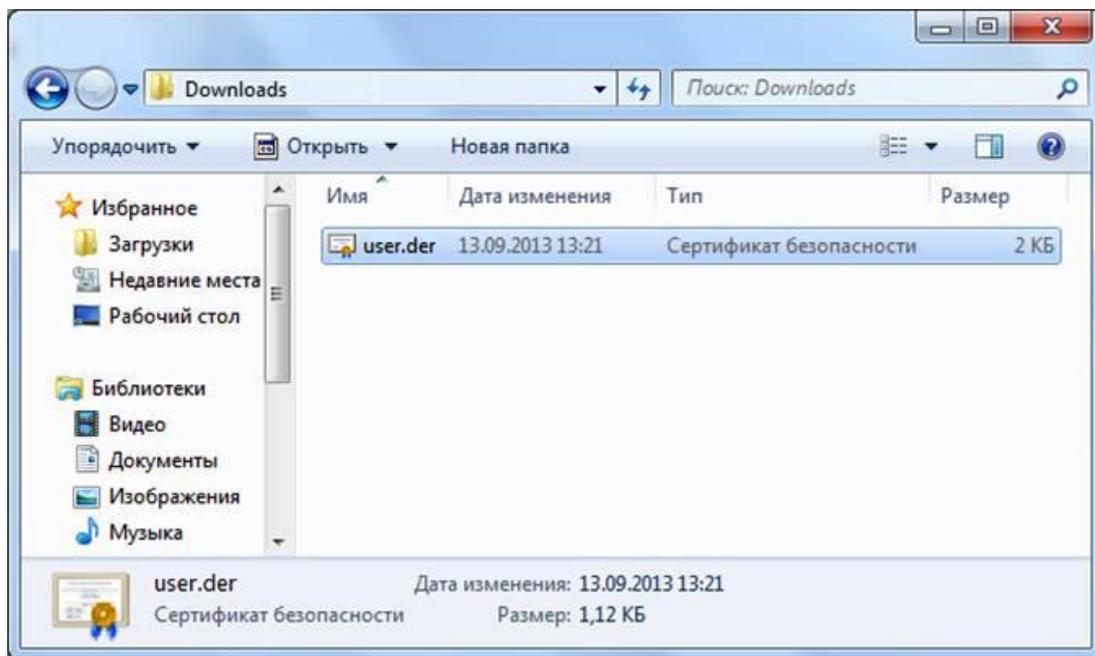


Рисунок Выбор файла сертификата

Откроется информация о сертификате. Нажмите на кнопку **Установить сертификат**:

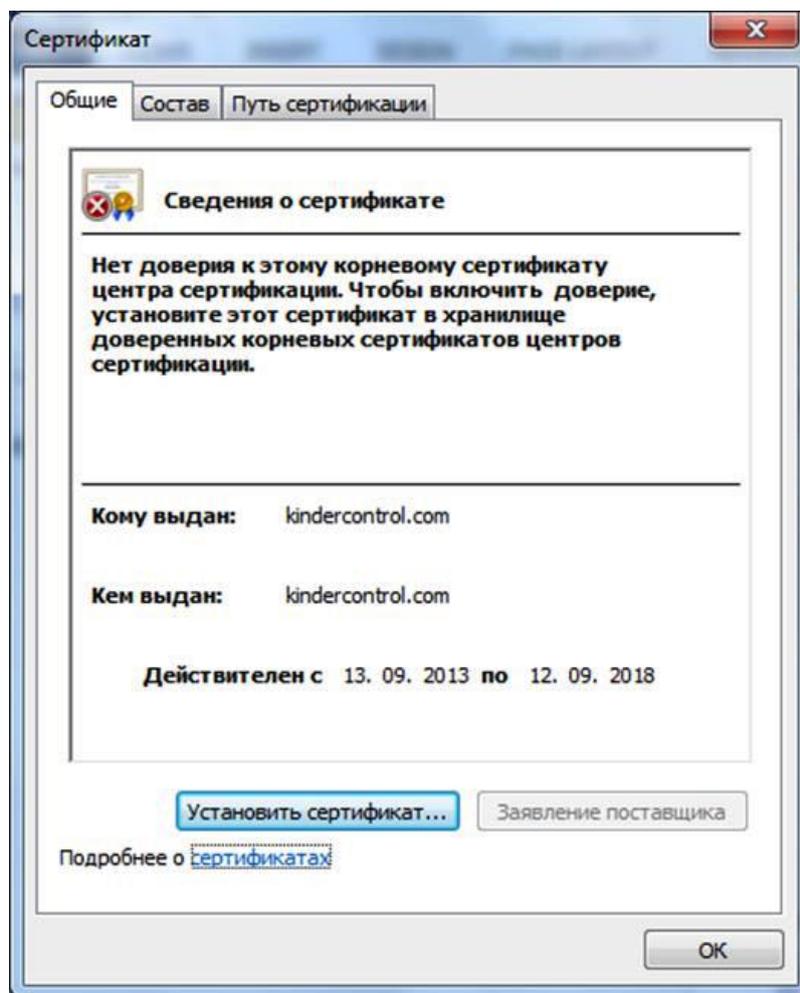


Рисунок Установка сертификата

Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:

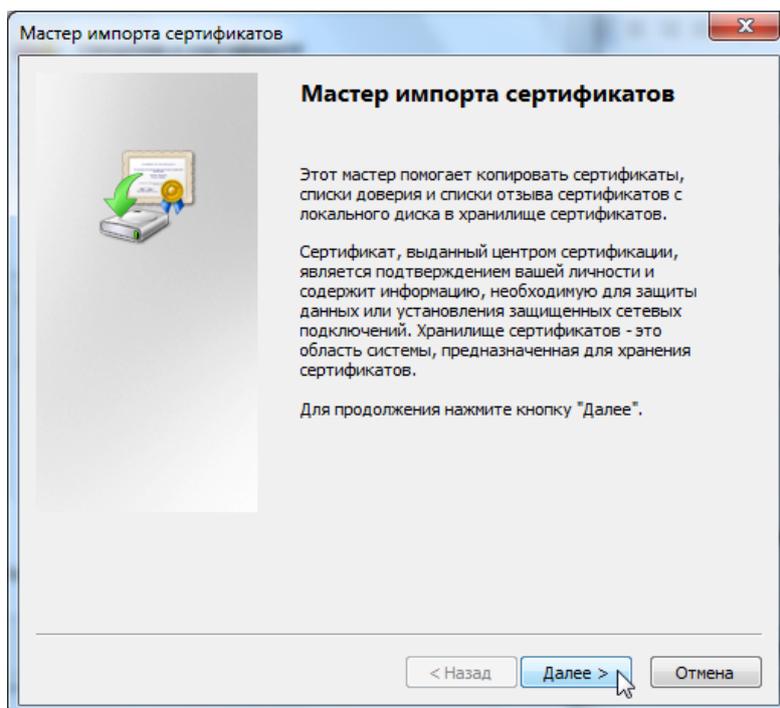


Рисунок Мастер импорта сертификатов

Выберите хранилище сертификата и нажмите кнопку **Обзор**:

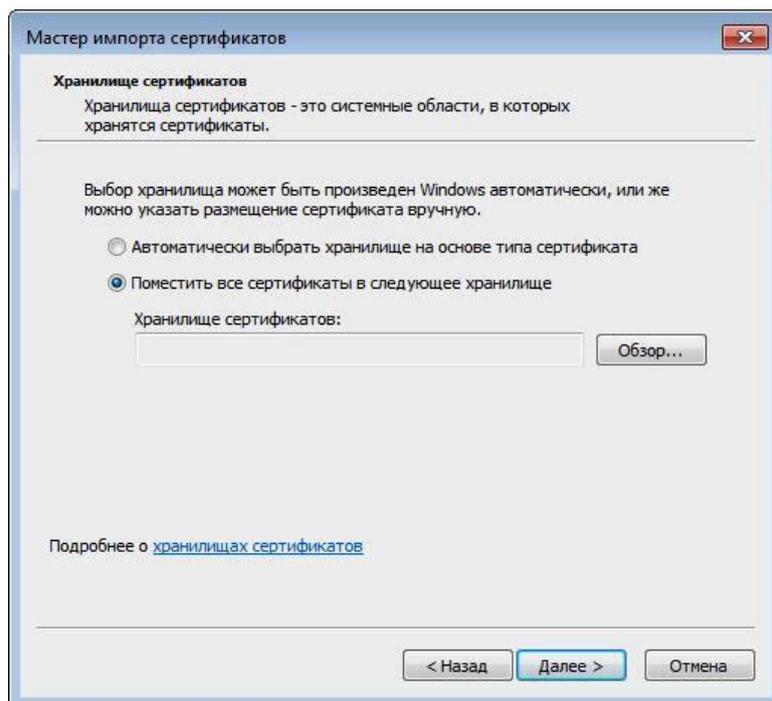


Рисунок Выбор хранилища

Выберите **Доверенные корневые центры сертификации** и нажмите кнопку **ОК**:

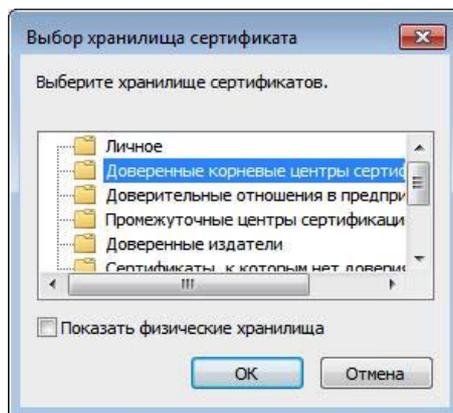


Рисунок Выбор хранилища (продолжение)

Нажмите кнопку «Готово»:

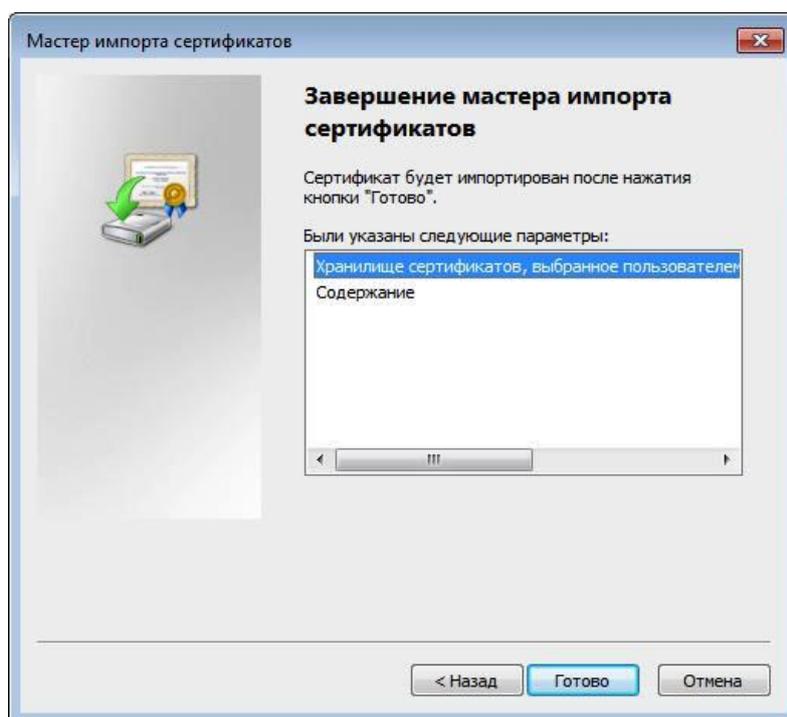
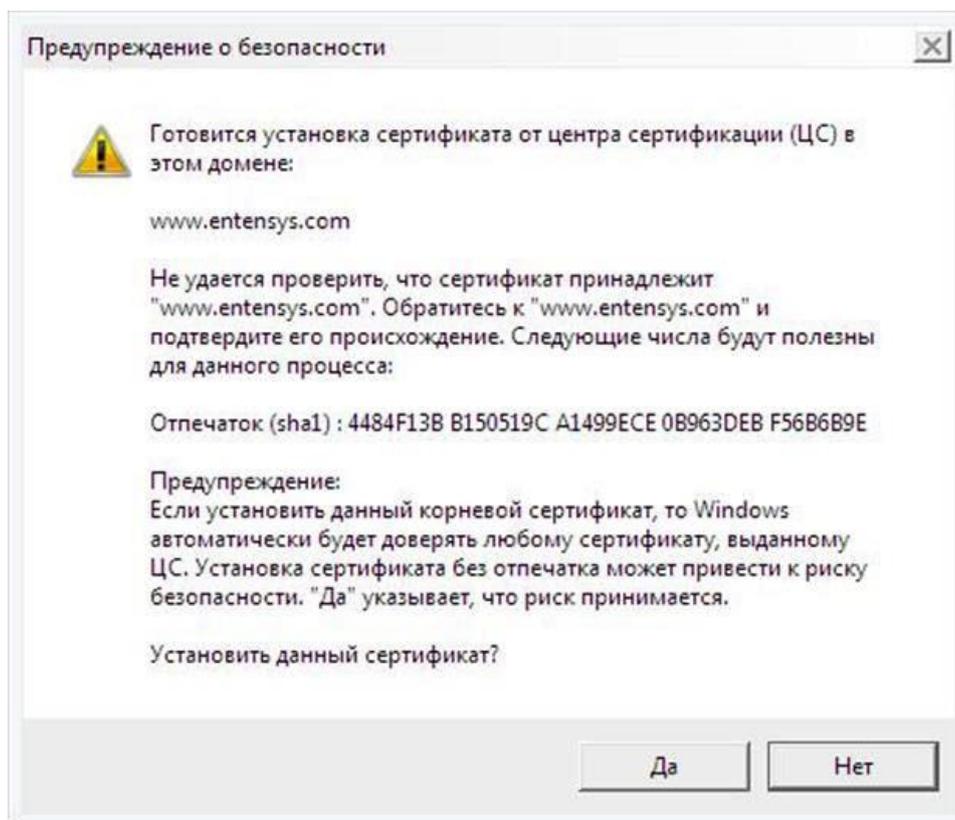
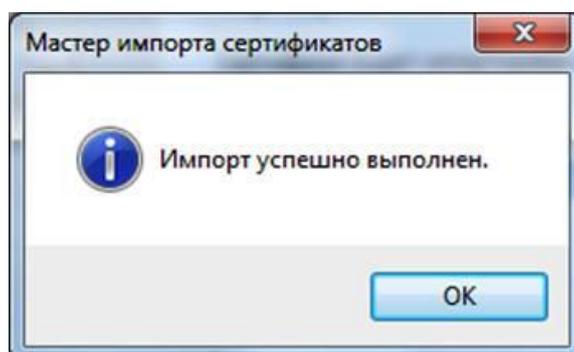


Рисунок Завершение импорта

Когда появится предупреждение системы безопасности, нажмите кнопку **Да**:



*Рисунок Согласие на установку сертификата*



*Рисунок Установка завершена*

Установка сертификата завершена.

## 18.2 Установка сертификата в браузер Safari, Chrome в ОС MacOSX

Перейдите в папку, куда вы скачали рет-сертификат и дважды нажмите на него:

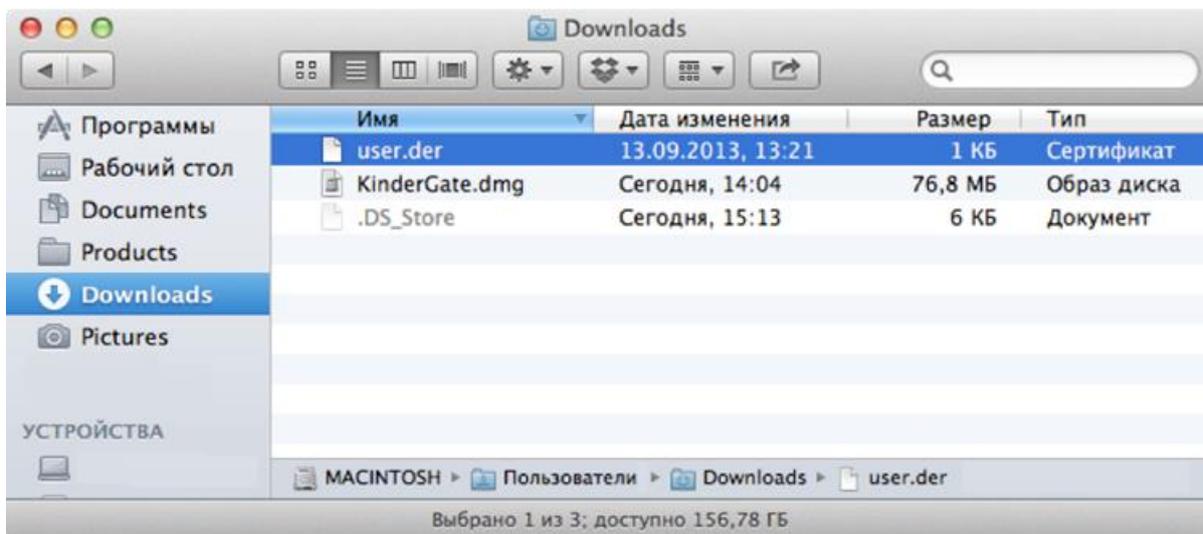


Рисунок Выбор файла сертификата

Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:

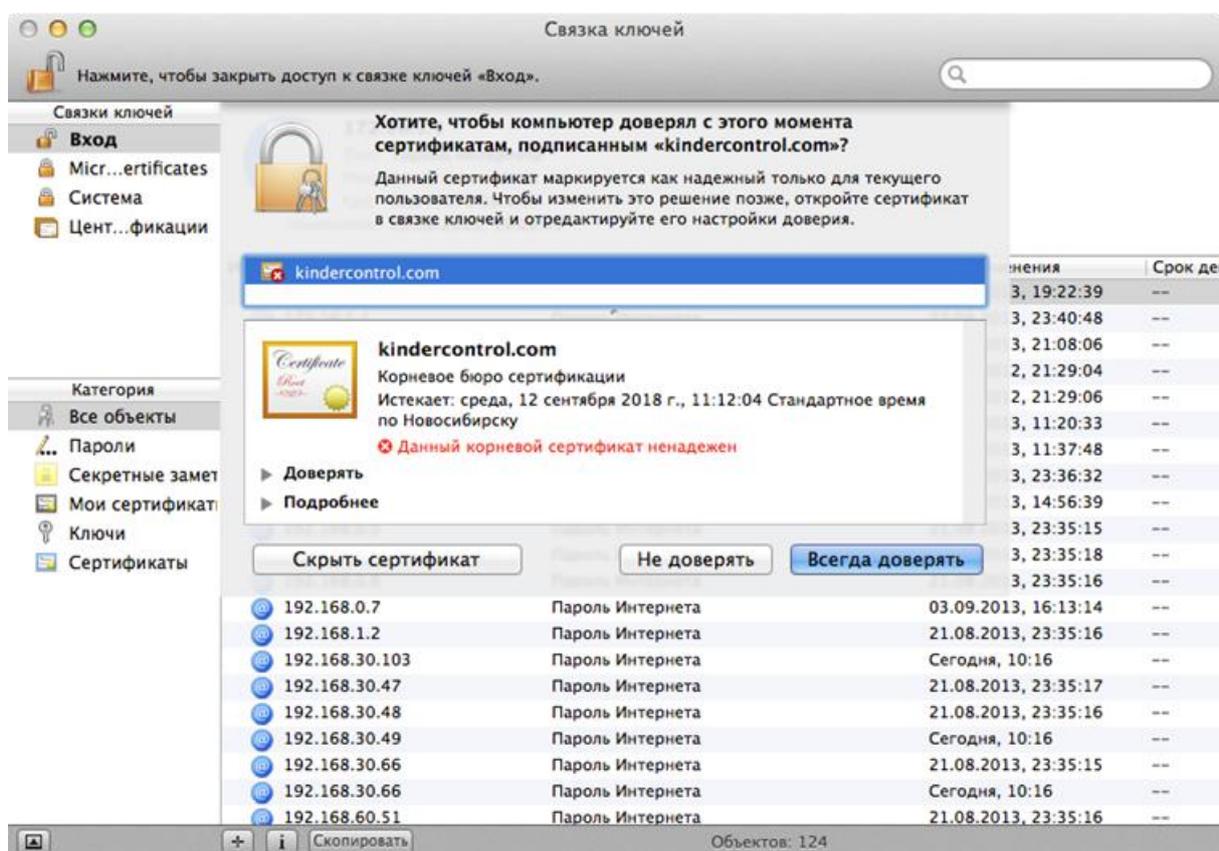


Рисунок Доверие сертификату

Введите свой пароль для подтверждения данной операции:

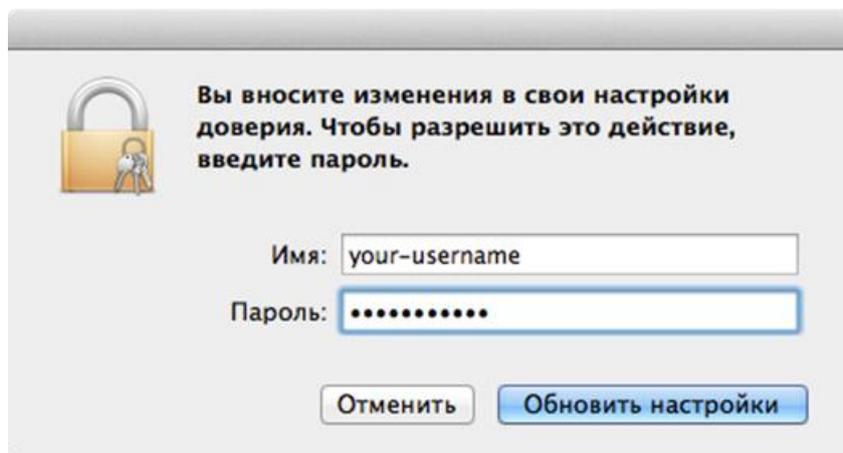


Рисунок Ввод пароля

Сертификат установлен.

### 18.3 Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется аналогично для всех операционных систем. Рассмотрим установку на примере ОС Windows.

Откройте настройки браузера Firefox (**Инструменты --> Настройки**):

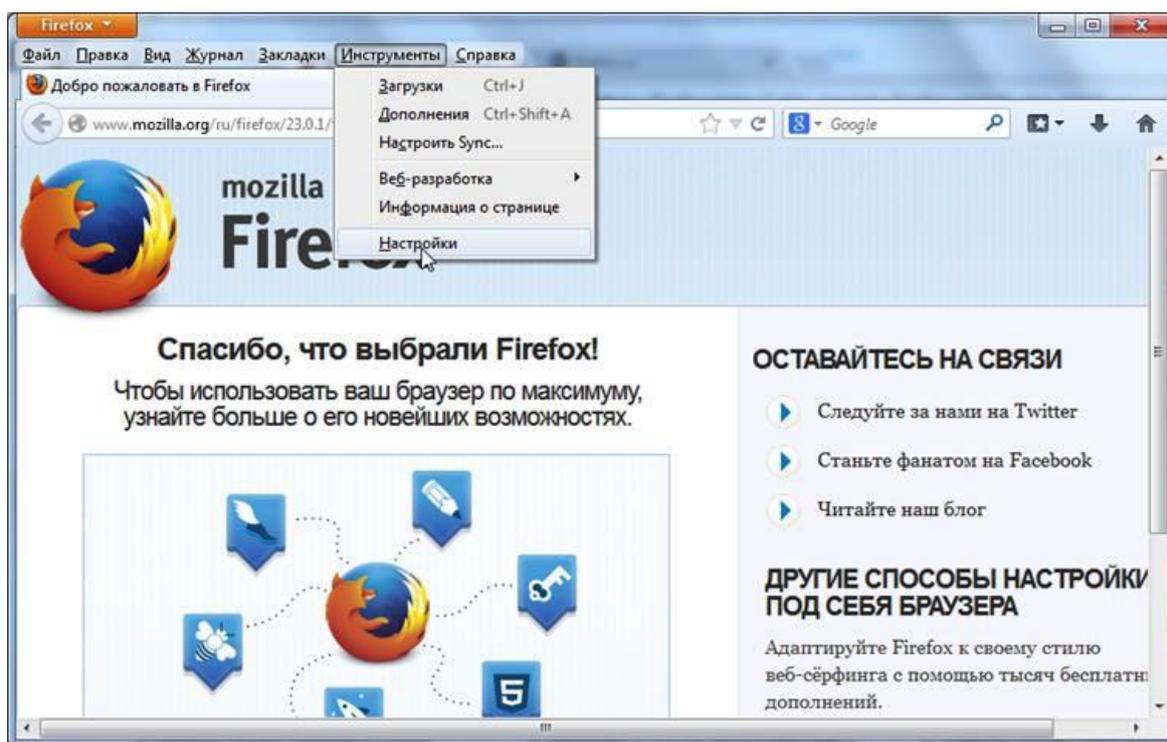


Рисунок Вход в режим Настройки

Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите на кнопку **Просмотр сертификатов**:

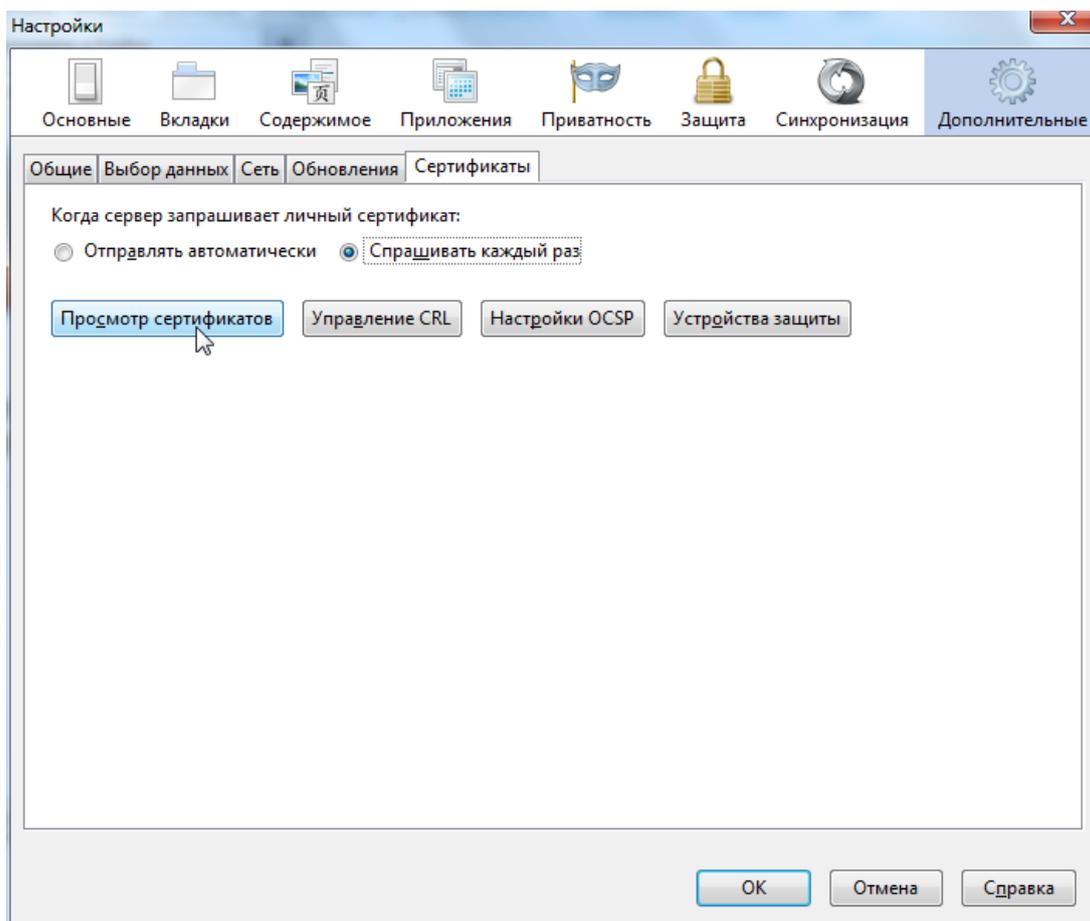


Рисунок Раздел Сертификаты

Нажмите кнопку **Импортировать** и укажите путь к скачанному pem-сертификату:

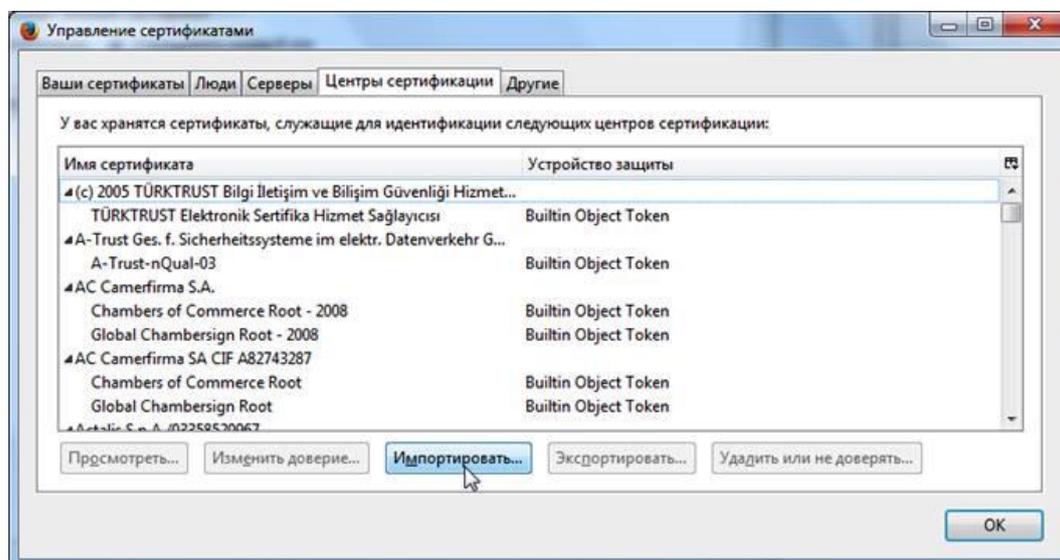


Рисунок Список установленных сертификатов

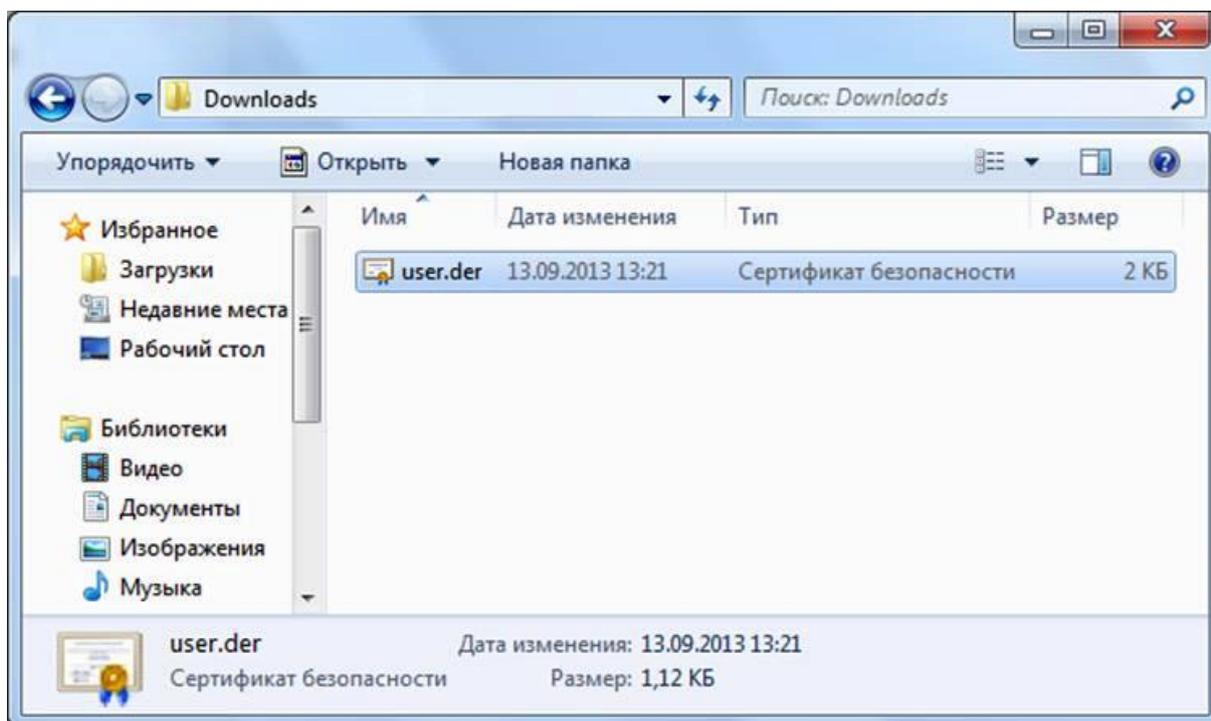


Рисунок Выбор файла сертификата

Установите галочку **Доверять при идентификации веб-сайтов** и нажмите **ОК**:

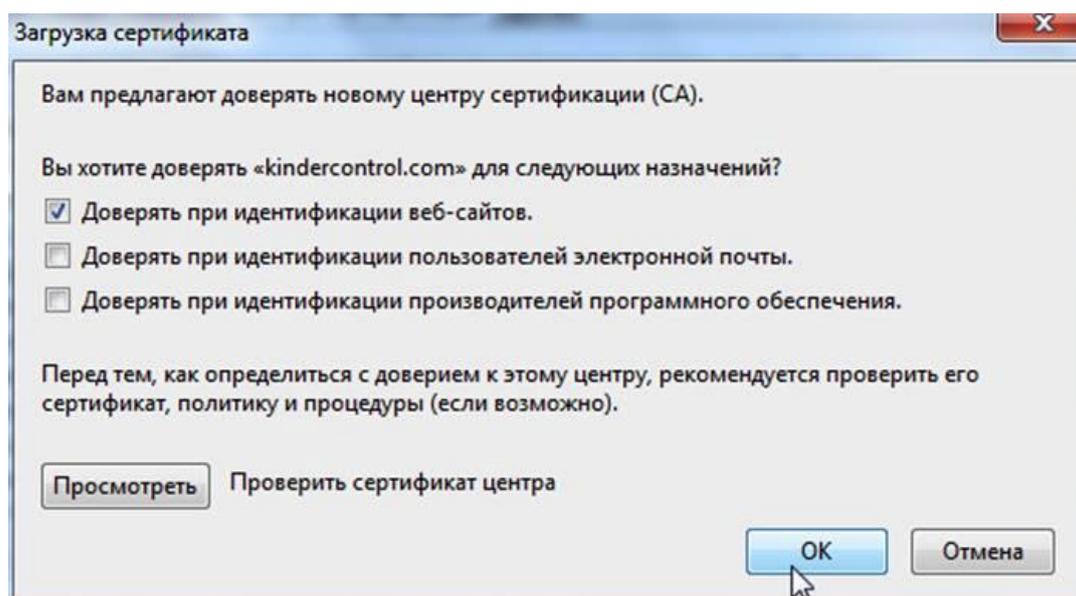


Рисунок Выбор типа доверия

Установка сертификата завершена.

## 19 ПРИЛОЖЕНИЕ №2. ТАБЛИЦА СООТВЕТСТВИЯ КАТЕГОРИЙ, УКАЗАННЫХ В ТРЕБОВАНИЯХ МИНИСТЕРСТВА ОБРАЗОВАНИЯ РФ К СКФ ДЛЯ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ, С КАТЕГОРИЯМИ USERGATE URL FILTERING 4.0.

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Peer-To-Peer	Пиринговые сети
Алкоголь. Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию	Алкоголь и табак
Баннеры и рекламные программы Баннерные сети, всплывающая реклама, рекламные программы	Реклама и всплывающие окна
Библиотеки	Искусство
Вождение и автомобили	Транспорт
Вредоносное программное обеспечение	Нелегальное ПО
Вредоносные программы	Ботнеты
	Сайты сомнительного содержания
	Вредоносное ПО
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечения	Поздравительные открытки
	Развлечения
	Мода и красота
	Отдых и оздоровление

	Рестораны и еда
	Спорт
	Путешествия
Здоровье и медицина	Здоровье и медицина
	Половое воспитание
Злоупотребление свободой СМИ - информация с ограниченным доступом. Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций	Оружие
Злоупотребление свободой СМИ - информация, содержащая скрытые вставки и иные технические способы воздействия на под-104№ п/п Тематическая категория Содержание скрытое воздействие сознание людей и (или) оказывающая вредное влияние на их здоровье	Сайты сомнительного содержания
Злоупотребление свободой СМИ - наркотические средства, сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Ненависть и нетерпение
	Насилие
Злоупотребление свободой СМИ -экстремизм Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы	Ненависть и нетерпение
	Насилие
Знакомства	Знакомства
Информация с ограниченным доступом. Информация, составляющая государственную или иную охраняемую законом тайну	Политика
	Правительство
Информация, пропагандирующая порнографию	Порнография и насилие
Компьютерные игры	Игры
Корпоративные сайты	Бизнес
	Финансы

Приложение №2. Таблица соответствия категорий, указанных в требованиях Министерства 201 / 204  
Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0.

	Общие
	Недвижимость
Корпоративные сайты, интернет-представительства негосударственных учреждений	Некоммерческие и неправительственные организации
Личная и немодерируемая информация. Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги	Персональные сайты
	Частные IP-адреса
	Социальные сети
	Потоковое мультимедиа и загрузки
	Веб-почта
Модерируемые доски объявлений (ресурсы данной категории, содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты	Социальные сети
	Чаты
Наркотические средства. Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Наркотики
Нелегальная помощь школьникам и студентам. Банки готовых рефератов, эссе, дипломных работ и пр.	Школьные мошенничества
Ненадлежащая реклама. Информация, содержащая рекламу алкогольной продукции и табачных изделий	Алкоголь и табак
Неприличный и грубый юмор. Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека	Сайты сомнительного содержания
Нижнее белье, купальники	Нудизм
Обеспечение анонимности пользователя, обход контентных фильтров. Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам	Анонимайзеры
	Переводчики

Приложение №2. Таблица соответствия категорий, указанных в требованиях Министерства 202 / 204 Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0.

Образовательные ресурсы	Образование
Онлайн-казино и тотализаторы	Азартные игры
Отправка SMS с использованием интернет-ресурсов. Сайты, предлагающие услуги по отправке SMS-сообщений	Реклама и всплывающие окна
Платные сайты	Паркованные домены
Поиск работы, резюме, вакансии	Поиск работы
Преступления - Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию)	Преступная деятельность
Преступления-клевета, экстремизм	Преступная деятельность
Программное обеспечение	Компьютеры и технологии
	Нелегальное ПО
	Информационная безопасность
Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения. Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение	Ненависть и нетерпение
Религии и атеизм	Религиозные культы
	Религия
Система поиска изображений	Обмен картинками
	Поисковые системы и порталы
СМИ	Форумы и новостные ленты
	Новости
Табак, реклама табака, пропаганда потребления табака. Сайты, пропагандирующие потребление табака; реклама табака и изделий из него	Алкоголь и табак
Торговля и реклама	Реклама и всплывающие окна

Приложение №2. Таблица соответствия категорий, указанных в требованиях Министерства 203 / 204  
Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0.

	Покупки
Убийства, насилие	Жестокое обращение с детьми
	Насилие
Чаты	Чаты
	Сервисы мгновенных сообщений
Экстремистские материалы или экстремистская деятельность (экстремизм)	Ненависть и нетерпение