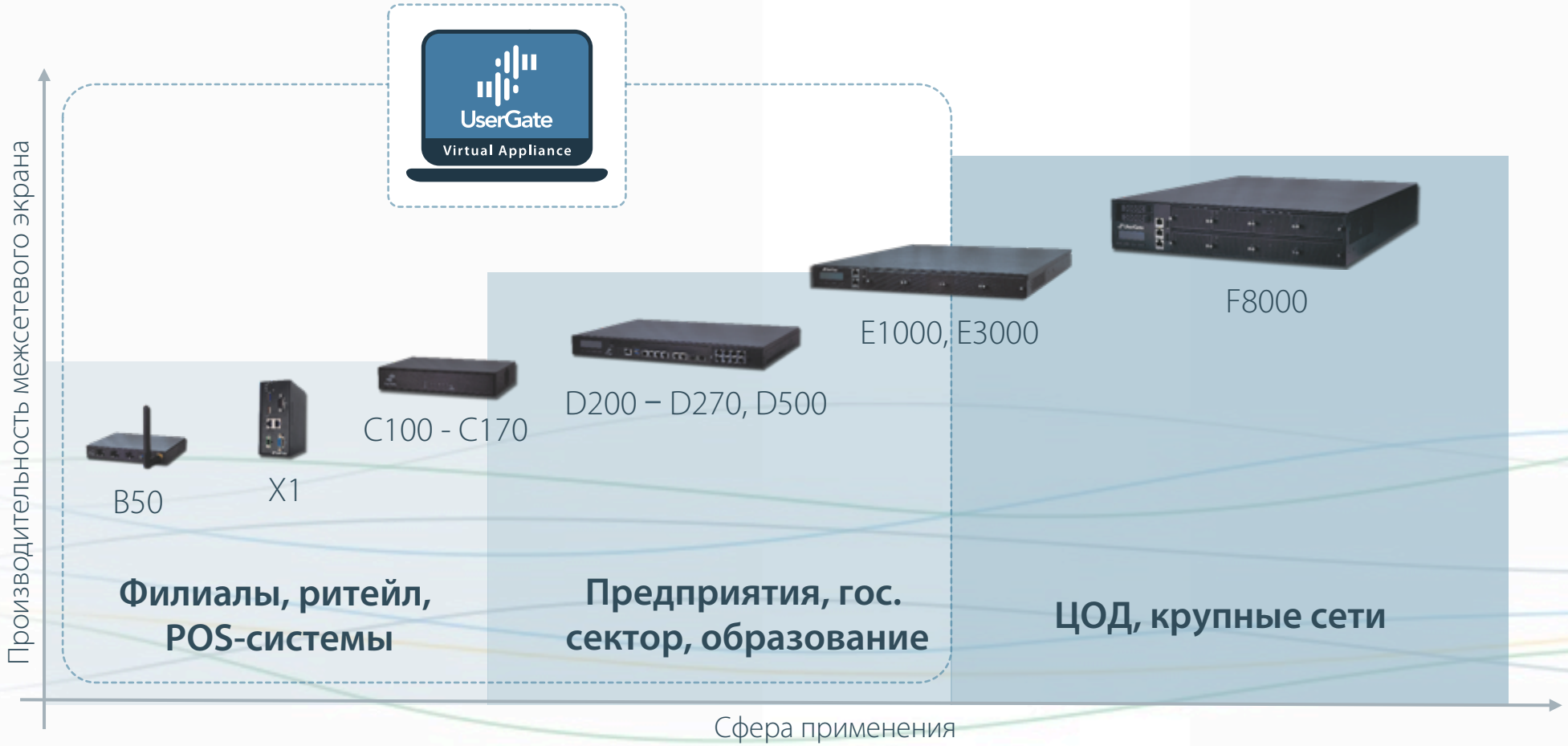
UserGate

Интернет-безопасность
для предприятий любого
размера

Наш офис разработки находится в Технопарке Новосибирского Академгородка, в месте, где тысячи талантливых разработчиков, инженеров, ученых занимаются производством высокотехнологичных продуктов.

Работа решений линейки UserGate основана на одноименной платформе, доступной в виде виртуального решения (готового образа для VMware, Hyper-V и прочих систем виртуализации) или в виде appliance, то есть программно-аппаратного комплекса.



vmware
VirtualBox
openstack
Hyper-V
Xen
KVM
Microsoft Azure
amazon web services

Характеристики аппаратных платформ

	UserGate B	UserGate C	UserGate D	UserGate E	UserGate F	UserGate X
Appliance						
FW, Гбит/с	0,25	До 1	18-20	25-30	40	0,3
IPS (COB), Мбит/с	10	100	500-700	1200-1500	4200	10
ATP, Мбит/с	15	50	300-350	400-600	2800	15
Контроль Приложений L7, Мбит/с	15	70	700-800	1000-1400	3200	15
Антивирус Касперского , Мбит/с	10	20	240-260	300-500	1000	8
Максимальное рекомендованное количество сессий	1-50	100	300-500	1000-3000	10000	-

Сфера применения

Филиалы, POS-системы, ритейл

VPN, МСЭ, СОВ, антивирус, антиспам

Предприятия, гос. сектор

МСЭ, Управление пользователям, управление трафиком, прокси-сервер

ЦОД, крупные сети

МСЭ, СОВ, антивирус UserGate, отказоустойчивость

Образовательные учреждения

контентная фильтрация, публичный WI-FI, соответствие требованиям ФЗ-139 и ФЗ-436

Объекты на открытом воздухе

VPN, МСЭ, СОВ, антивирус, SCADA

UserGate

Сфера применения

Здравоохранение

Банки и финансовые организации

Горнодобывающая промышленность

Наука

Энергетика и топливно-энергетический комплекс

Транспорт

Металлургическая промышленность

Сфера атомной энергии

Химическая промышленность

Связь

Ракетно-космическая промышленность

Оборонная промышленность

О решениях на платформе UserGate

Операционная система UG OS

UserGate работает на базе специально созданной и поддерживаемой операционной системы, а также на специально спроектированных аппаратных устройствах, позволяющих обеспечить наибольшую эффективность и скорость обработки трафика.

Разработчики уделили много внимания созданию собственной платформы, не основанной на использовании чужого исходного кода и сторонних модулей. Это позволяет обеспечивать высокое качество продукта, надежность работы, а также его скорейшее развитие и возможность адаптации для самых сложных проектов.

Защита от угроз

Защита от угроз нулевого часа

В платформе UserGate используются технологии поведенческого анализа, оценка репутации всевозможных ресурсов, доступ к базам сигнатур известных вредоносных программ, а также «песочницам».

Защита от DoS-атак

На базе платформы UserGate возможно обеспечить защиту от DoS-атак, в том числе ограничивая максимальное число соединений на одного пользователя.

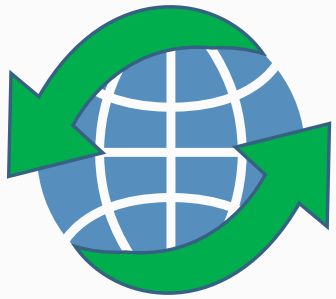
Блокировка рекламы

UserGate анализирует загружаемый контент с учетом знания известных рекламных сетей и используемых ими скриптов.

Разбор и анализ трафика

UserGate осуществляет морфологический анализ содержимого веб-страниц на наличие определенных слов и словосочетаний (Web 2.0).

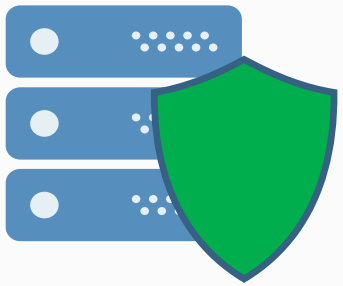
Анализ угроз (Поддержка концепции SOAR)



Технологии, используемые в UserGate, соответствуют современной концепции SOAR (Security Automation, Orchestration and Response), позволяют анализировать поведение различных процессов, выявлять риски и автоматически обеспечивать на основе этого анализа адекватную реакцию, обеспечивая защиту от угрозы или просто от аномального поведения на самой ранней стадии.

Администратор может задавать сценарии и ответные действия на события, что сокращает время между обнаружением угрозы и ответом на нее, а также приоритезировать события, обеспечивая своевременную реакцию на критические атаки.

Защита от атак, безопасность дата-центров



Система обнаружения и предотвращения вторжений (IPS - Intrusion Prevention System) позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.

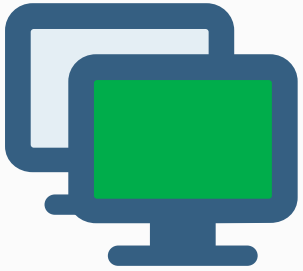
Выявление проблем безопасности происходит с помощью использования эвристических правил и анализа сигнатур известных атак. Система IPS отслеживает и блокирует подобные атаки в режиме реального времени. Возможными мерами превентивной защиты являются блокирование определенных сегментов сетевого трафика, обрыв соединения и оповещение администратора сети.

Безопасность почты

Проверка почты важна как для фильтрации спама, так и для защиты от зараженных писем, фишинга, фарминга и прочих видов мошенничества.

UserGate позволяет отфильтровывать письма, основываясь на анализе их содержания и эвристике. Анализу подвергаются письма на любых языках, а также графические сообщения. При этом обеспечивается практически нулевой уровень ложной детекции. Центр обнаружения спама выявляет спамерские атаки в любой точке мира.

Виртуальная частная сеть (VPN)



UserGate позволяет использовать VPN как для удаленного подключения устройств, так и для создания защищенных туннелей между серверами. Такой подход позволяет объединить разрозненные офисы в единую логическую сеть, значительно сокращая и упрощая применение единых настроек безопасности в сети филиалов.

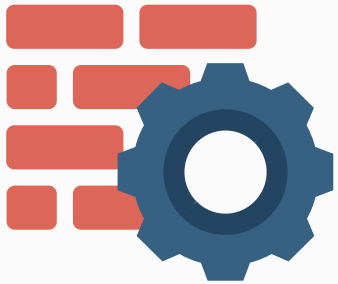
Это позволяет обеспечить безопасный доступ к корпоративным ресурсам для сотрудников компаний с распределенной структурой.

Интернет-фильтрация

Использование интернет-фильтрации значительно увеличивает безопасность локальной сети, так как позволяет обеспечить административный контроль за использованием интернета, закачками и обеспечивает блокировку посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой.

UserGate получил ряд наград именно за качество интернет-фильтрации и широко используется для этой цели во многих организациях, вузах и у операторов связи.

Корпоративный межсетевой экран



Решение UserGate обеспечивает межсетевое экранирование для средних и крупных предприятий, поддерживая высокую скорость обработки трафика, многоуровневую безопасность, применение гранулярных политик к пользователям и прозрачное использование интернет-канала.

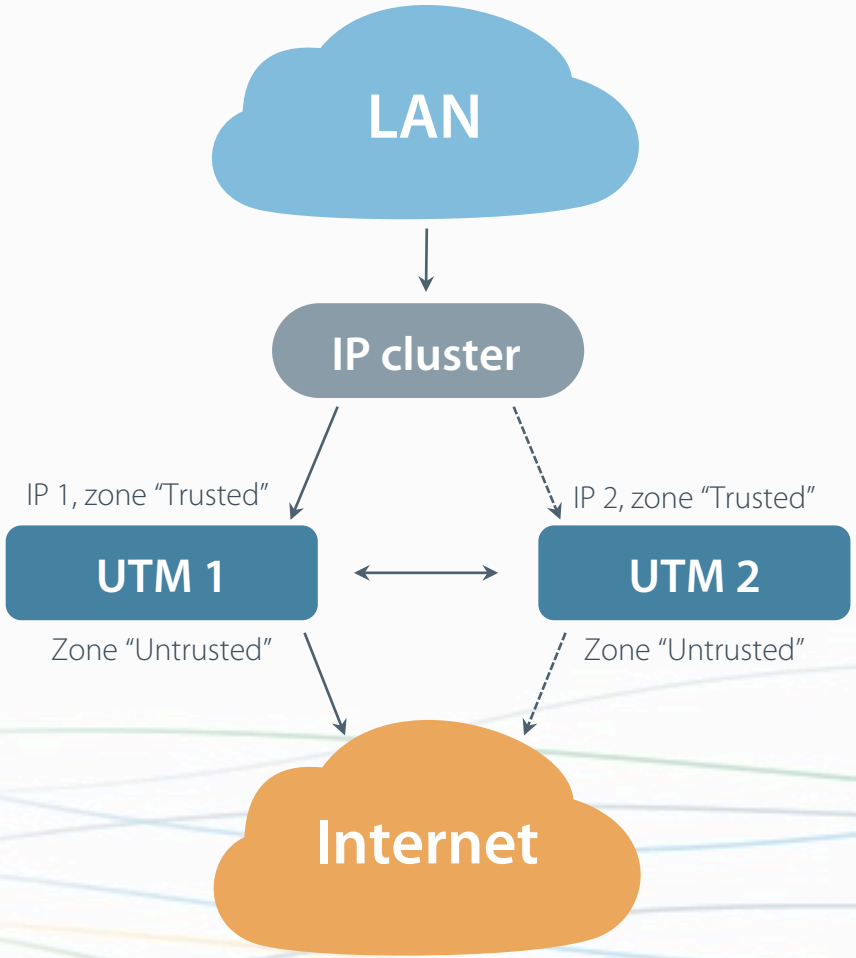
Работа функций безопасности основана на постоянном взаимодействии с нашим центром безопасности, что позволяет поддерживать минимальное время реакции на разнообразные современные угрозы.

Высокая отказоустойчивость и кластеризация

Функция высокой отказоустойчивости (High Availability) позволяет кардинально снизить риски, которые могут возникать в связи со сбоями в работе аппаратного обеспечения, на котором установлен UserGate. Данная функция позволяет устанавливать систему на парных узлах и автоматически переключать между ними нагрузку в случае сбоев.

В решении реализована поддержка кластеризации в режиме active-active и active-passive. Кластеризация позволяет применять к разным нодам единые настройки, политики, библиотеки, сертификаты, сервера авторизации, группы пользователей и т. д.

Использование в высоконагруженных системах



UserGate поддерживает возможность кластеризации, а также режим высокой доступности (High Availability).

Кластеризация позволяет применять к разным нодам единые настройки, политики, библиотеки, сертификаты, сервера авторизации, группы пользователей и т. д.

Другие функции

Поддержка АСУ ТП (SCADA)

Контроль доступа в интернет

Гостевой портал

Контроль приложений на уровне L7

Безопасная публикация ресурсов и сервисов

Идентификация пользователей

Дешифрование SSL

Антивирусная защита

Контроль мобильных устройств, поддержка концепции BYOD

Поддержка АСУ ТП (SCADA)

В обновленной версии операционной системы UG OS появилась возможность настройки автоматизированной системы управления технологическим производством (АСУ ТП, SCADA) и управления ей. Таким образом, администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий.

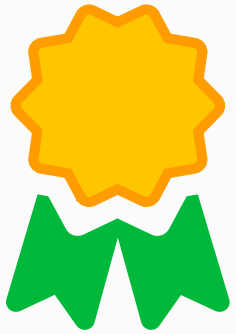
Это позволяет автоматизировать основные операции технологического процесса, сохраняя при этом возможность контроля и вмешательства человека при необходимости.

Контроль приложений на уровне L7

Функция контроля приложений (на уровне L7) на основе обновляемых баз сигнатур может быть использована в правилах межсетевого экрана и правилах пропускной способности.
Это обеспечивает защиту от угроз, связанных с программами, имеющими доступ в интернет.

Данная функции с одной стороны позволяет администраторам ограничивать использование таких приложений, как мессенджеры или торрент-клиенты, в личных целях, с другой - защитить локальную сеть от связанных с интернетом угроз.

Дешифрование SSL



Наряду с обычным нешифрованным трафиком UserGate может быть настроен и для фильтрации HTTPS-трафика. При этом сервер на лету осуществляет подмену сертификата и использует полный набор методов фильтрации, включая морфологическую контент-фильтрацию.

Контроль доступа в интернет

UserGate обеспечивает контроль работы веб-приложений и доступа в интернет с помощью создания правил, основанных на персонализированной политике. Это обеспечивает разноуровневый доступ к сетевым ресурсам и позволяет распределять ширину канала между различными приложениями и сервисами.

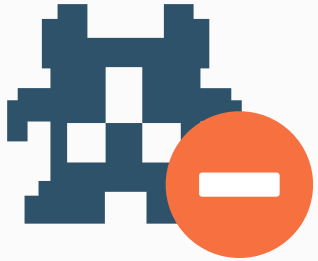
Функция контроля доступа в интернет также позволяет автоматически применять настройки безопасности к отдельным пользователям и объектам сетевой инфраструктуры.

Безопасная публикация ресурсов и сервисов

UserGate обеспечивает безопасность корпоративной сети, блокируя возможность несанкционированного проникновения извне. Однако в определенных случаях важно обеспечить внешний доступ к корпоративным ресурсам, а также к сервисам, запущенным на серверах внутри корпоративной сети.

UserGate можно использовать для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.

Антивирусная защита



В UserGate предоставляет различные способы обеспечения антивирусной проверки трафика.

Антивирус UserGate, включаемый в дополнительный модуль Advanced Threat Protection, обеспечивает быструю проверку трафика на наличие вредоносного кода путем анализа сигнатур получаемых файлов и приложений. Данный метод антивирусной проверки практически не влияет на производительность системы.

Встроенный антивирусный модуль от Лаборатории Касперского предоставляет более сложную проверку трафика.

Гостевой портал

UserGate позволяет обеспечить гостевой интернет-доступ через Wi-Fi. При этом поддерживаются различные методы аутентификации – в том числе по одноразовому паролю, а также через SMS.

Возможно применение к гостевым пользователям специальных политик и правил, обеспечение мониторинга использования интернета и получение данных статистики.

Идентификация пользователей

UserGate поддерживает аутентификацию пользователей и применение к пользователям правил межсетевого экранирования, контентной фильтрации, контроля приложений с поддержкой таких средств и протоколов аутентификации, как Active Directory, Kerberos, RADIUS, LDAP, Captive Portal, TACACS+, 2FA.

Администраторы могут применить определенные политики безопасности к любому пользователю, группе пользователей или, например, ко всем неизвестным пользователям.

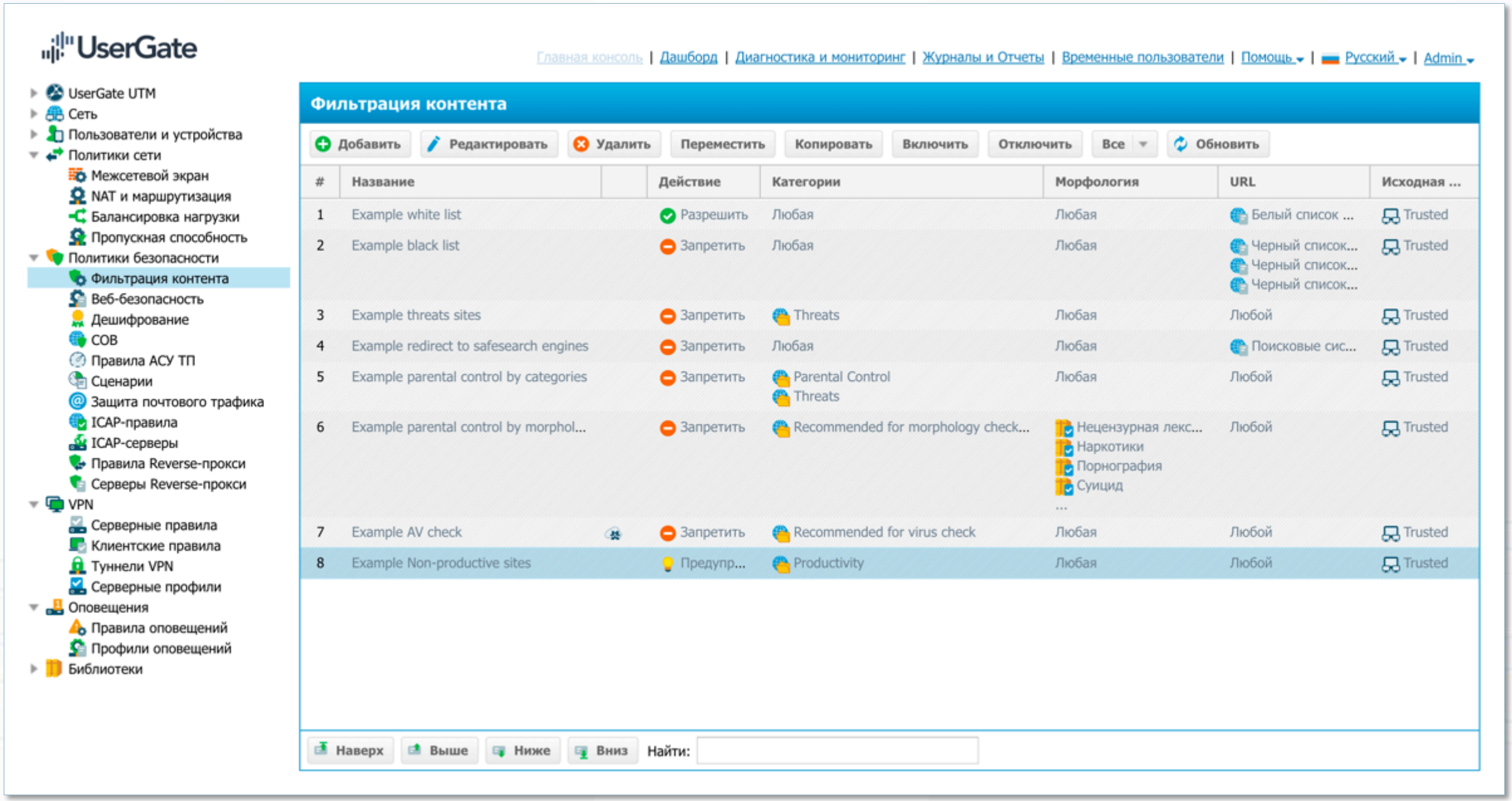
Контроль мобильных устройств

Возможно применение специальных правил доступа к любым устройствам, включая ноутбуки, планшеты, смартфоны, используемым пользователями.

UserGate позволяет устанавливать ограничения на максимальное число устройств на одного пользователя (общее и одновременно используемых), а также задать список конкретных устройств, которые пользователь может использовать для получения доступа в сеть.

Поддержка концепции BYOD (Bring Your Own Device)

Консоль управления



Лицензирование

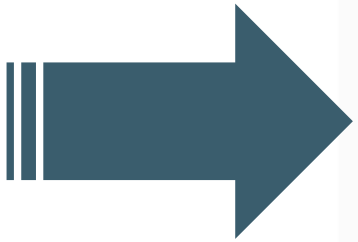
UserGate лицензируются по количеству одновременно использующих его пользователей, точнее IP- адресов, с которых подключаются устройства пользователей.

Дополнительно ежегодно лицензируются следующие модули:

- **Security Updates**. Включает обновления ПО UserGate, обновления операционной системы, баз сигнатур вторжений и известных приложений (L7), а также техническую поддержку.
- **Advanced Threat Protection**. Включает подписку на использование баз DNS-фильтрации, морфологических словарей и антивируса UserGate, определяющего репутацию файлов.
- **Kaspersky Antivirus**. Включает подписку на антивирусный модуль Лаборатории Касперского.
- **Mail Security**. Включает подписку на антиспам.

* В базовую лицензию включена годовая подписка на Security Updates

Импортозамещение



UserGate

Конкурентное окружение

Зарубежные решения

Check Point, Cisco, Dell SonicWALL, Fortinet, Juniper Networks, McAfee, Sophos, WatchGuard, Barracuda Networks, Palo Alto Networks, StoneSoft

Зарубежные решения на данный момент серьезно доминируют на российском рынке во всех сферах, кроме тех, где требуются сертификаты ФСБ.

Российские альтернативы

Инфотекс, Код Безопасности, Alltel

Отечественные решения серьезно уступают в плане функциональности и производительности. Единственные их применения – это использование для работы с гостайной и организация VPN-соединений с ГОСТ-шифрованием

Сертификат ФСТЭК № 3905

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3905

Выдан 26 марта 2018 г.
Действителен до 26 марта 2021 г.

Настоящий сертификат удостоверяет, что **изделие «Универсальный шлюз безопасности «UserGate UTM»**, разработанное и производимое ООО «еСЛ Девелопмент», является системой обнаружения вторжений и межсетевым экраном, соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре 643.95486689.UTM-01 30.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СИ RU.0001.01БИ00.Б010) - техническое заключение от 07.02.2018, экспертного заключения от 15.02.2018 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СИ RU.0001.01БИ00.А002).

Заявитель: ООО «еСЛ Девелопмент» (ИНН 5408243746)
Адрес: 630090, г. Новосибирск, ул. Николаева, д. 11, оф. 602,
Телефон: (383) 286-2913

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляются испытательной лабораторией АО «НПО «Эшелон».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 26 марта 2018 г.

Решение UserGate успешно прошло сертификацию ФСТЭК по требованиям к Межсетевым Экранам (4-й класс, профили А и Б) и по требованиям к Системам Обнаружения Вторжений (4-й класс) для программно-аппаратных (модели UserGate C, D, D+, E, E+, F, X1) и виртуальных платформ UserGate.

Данный уровень сертификации дает возможность использования решения в составе автоматизированных систем до класса защищенности 1Г, информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС) до 1 класса (уровня) защищенности включительно, т. е. не обрабатывающих гостайну. Решение полностью удовлетворяют требованиям 17 и 21 приказов ФСТЭК для обработки персональных данных 1-4 категорий.

Часто задаваемые вопросы

- **Сроки поставки решения?**

ПО поставляется разу после оплаты, аппаратная часть отгружается в течение 3-5 дней (при наличии на складе).

- **Оборудование?**

Мы предлагаем 6 видов аппаратных платформ собственной сборки (РФ).

- **Какой антивирус выбрать?**

Антивирус UserGate менее требователен к ресурсам аппаратной платформы и достаточно эффективен согласно актуальной сигнатурной базе. Антивирус Касперского позволяет проводить дополнительный эвристический анализ трафика, но при этом требует больше ресурсов.

- **Возможность создания собственных black/white list?**

Решение UserGate дает возможность создавать черные и белые списки самостоятельно.

Часто задаваемые вопросы

- **Фильтрация HTTPs?**

Решение UserGate позволяет производить инспекцию, дешифрацию SSL-трафика, также осуществляет подмену сертификатов (MitM), соответственно весь зашифрованный SSL трафик возможно анализировать также как и не шифрованный.

- **Российская компания?**

ООО «Юзергейт» Российская компания, не имеющая иностранных инвестиций, основанная в 2001 году в г.Новосибирске.

- **Реестр Российского ПО?**

Решение UserGate включено в Единый Реестр Российского ПО.

(Рег. номер ПО:1194 в реестре Минкомсвязи)

Защита органов власти от интернет-угроз

Департамент информационных Технологий Ханты-Мансийского автономного округа — Югры

Задачи:

- Замена зарубежного решения
- Обеспечение функций прокси-сервера
- Интернет-фильтрация

Решение:

- Виртуальная платформа UserGate
- Модуль ATP (расширенная защита от угроз нового поколения)

> *«Мы убедились, что UserGate является надежным, удобным и функциональным решением, ни в чем не уступающим известным нам зарубежным решениям», – заявил директор Бюджетного учреждения «Окружной центр ИКТ» Степан Перевертайло.*

Платформа UserGate обладает всеми функциями межсетевого экрана нового поколения и не уступает мировым лидерам, таким как Check Point, Fortinet, Palo Alto Networks

Платформа UserGate – это:

- Межсетевой экран нового поколения
- Обеспечение безопасности на уровне приложений (L7)
- Система обнаружения вторжений
- Поведенческий анализ потенциальных угроз
- Автоматическая реакция на неизвестные угрозы
- Применение гранулярных политик к пользователям
- Разбор защищенных протоколов (SSL)
- Глубокий анализ содержимого, загружаемого из интернета (DCI)

UserGate

Нас выбирают:

ПРАВИТЕЛЬСТВО МОСКВЫ

ПЕНСИОННЫЙ ФОНД РОССИЙСКОЙ ФЕДЕРАЦИИ

Ростелеком

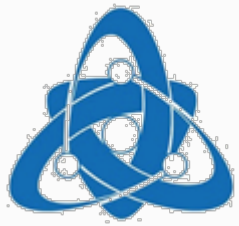
MEGAFON

VIVACELL

MTS

ҚАЗАҚТЕЛЕКОМ

Нас выбирают:



РОСЭНЕРГОАТОМ
РОСТОВСКАЯ АЭС

ФОСАГРО

Транснефть

Heathrow

lady & gentleman
CITY

Лада-Имидж
Акционерное общество

Нас выбирают:

В группе компаний Фосагро UserGate используется для доступа в сеть.
На всех доменных ПК используется SSO и авторизация Kerberos, в основном офисе более 2000 пользователей. Для авторизации при подключению к публичному гостевому WiFi используется Captive Portal.

Основная задача, решаемая UserGate состоит в сложной фильтрации http/https трафика по определённым группам пользователей, запрет интернет ресурсов по категориям, антивирусная проверка трафика на уровне шлюза, фильтрация по спискам. Все эти меры обеспечивают эффективное использование интернет-ресурсов сотрудниками компании.

По просьбе заказчика была реализована возможность отправлять весь входящий в UserGate трафик по протоколу ICAP на сервер с DLP (SearchInform) для дальнейшего анализа. Также была расширена информация передаваемая по ICAP на DLP сервер, добавлена информация о неавторизованных пользователях – по IP и MAC-адресу.

В УрГУПС используется интернет-канал с пропускной способностью 1Гб/с, обеспечивающим одновременное подключение 4000 пользователей

В настоящее время УрГУПС использует UserGate для фильтрации публичного WiFi с авторизацией по SMS как по категориям, так и по контенту. Также настроена система обнаружения вторжений СОВ (IPS), успешно блокируются пиринговые P2P сети и определенные приложения (на уровне L7).

Суммарная нагрузка на уровне шлюза составляет более 400 Мб/с.

lady & gentleman CITY

В компании была настроена защищенная с помощью UserGate сеть Wi-Fi, использующая аутентификацию через Captive Portal.

Вместе базовой лицензией на UserGate был приобретен дополнительныи модуль Advanced Threat Protection, обеспечивающий защиту от современных угроз и блокировку разнообразного опасного контента, вредоносных приложений, скриптов.

UserGate также предоставил возможность блокировки определенных ресурсов, осуществления мониторинга использования интернета, получения исчерпывающей статистики и применение групповых политик.

«Мы потратили совсем немного усилий на установку и настройку UserGate. Данное решение зарекомендовало себя как надежное и стабильное, обеспечивающее полноценную интернет-безопасность без негативного влияния на скорость доступа.», – говорит системныи инженер сети lady & gentleman CITY Першин Евгений Дмитриевич.

Награды

В подтверждение высокого качества UserGate стал финалистом конкурса SC Awards 2014 американского журнала SC Magazine наравне с WebSense, Barracuda, Fortinet и ClearSwift и победителем SC Awards 2015 SC Magazine Awards Europe британского издания SC Magazine, опередив в финале Trustwave, Websense и Barracuda Networks.

В феврале 2017 года UserGate вошел в пятерку лучших UTM-решений года.

https://www.scmagazine.com/sc-awards-finalists-2017-round-six/article/572883/

UserGate

Спасибо за внимание

www.usergate.ru | sales@usergate.ru