

Линейка решений UserGate

Операционная система UGOS

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 работы продукта, а также его скорейшее развитие и адаптацию для самых сложных проектов.



Соответствие законодательству РФ

Сертификат ФСТЭК России № 3905:

- Приказ ФСТЭК России № 76 от 02.06.2020 по 4 УД
- ИТ.МЭ.А4.ПЗ

- ИТ.МЭ.Б4.ПЗ
- ИТ.МЭ.Д4.ПЗ
- ИТ.СОВ.С4.ПЗ

Внесен в Единый реестр российских программ для ЭВМ и БД (запись 1194)



Защита от угроз и атак

Защита от угроз нулевого часа

Сочетание самых разных технологий позволяет добиться максимально быстрой реакции на возникновение новых угроз. UserGate обеспечивает лучшую защиту от так называемых угроз «нулевого часа», а также позволяет предотвращать нарушение приватности пользователя со стороны различных поисковых машин, социальных сетей и других компаний.

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

Блокировка рекламы

Модуль Adblock анализирует загружаемый контент с учетом знания известных рекламных сетей и используемых ими скриптов. Это позволяет блокировать рекламный контент, подгружаемый со сторонних сайтов, а также всплывающие окна.

UserGate также может блокировать скрипты, которые обеспечивают наблюдение за поведением пользователя в интернете.

Защита от DoS-атак

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

Разбор и анализ трафика

UserGate осуществляет морфологический анализ содержимого веб-страниц на наличие определенных слов и словосочетаний. Это позволяет контролировать доступ к конкретным разделам сайта, не блокируя ресурс целиком на уровне категории или домена. Подобный подход актуален для различных социальных сетей, форумов и других порталов, в наполнении которых значительную роль играют пользователи (Web 2.0).

В UserGate реализована технология Deep Content Inspection (DCI), которая является развитием технологии Deep Packet Inspection (DPI). Это позволяет обеспечить полный прозрачный разбор и анализ трафика, передаваемых данных, текстов на самом высоком уровне – уровне анализа самого содержимого, а не пакетов или приложений.

Решение использует специальные морфологические словари, составленные на основе требований законодательства РФ.



Межсетевой экран нового поколения

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 современные угрозы.



Интернет-фильтрация (Internet filtering)

Использование интернет-фильтрации значительно увеличивает безопасность локальной сети, так как позволяет обеспечить административный контроль за использованием интернета, загрузками, блокирует 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, в число которых входят крупные ВУЗы и операторы связи.



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.



Безопасность почты (Mail Security)

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. 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.



Безопасность дата-центров (IDS/IPS)

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 атаки в режиме реального времени. Возможными мерами превентивной защиты являются блокирование определенных сегментов сетевого трафика, обрыв соединения и оповещение администратора.



Кластеризация и высокая отказоустойчивость

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 группе узлов 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.



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.

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.

UserGate C

Модели: C100



Производительность
межсетевого экрана
до 2 Гб/с

Устройство UserGate C100 является компактным и удобным в настройке сетевым устройством и обеспечивает эффективную защиту от угроз.

Для малого бизнеса, филиалов, POS-систем, ритейла, образования

UserGate D

Модели: D200 | D500



Производительность
межсетевого экрана
до 20 Гб/с

UserGate серии D является полноценным сетевым сервером, способным обеспечить безопасность предприятий небольшого и среднего размера с несколькими сотнями пользователей.

Для среднего бизнеса, образования, медицины, государственных структур и крупных филиалов

UserGate E

Модели: E1000 | E3000



Производительность
межсетевого экрана
до 30 Гб/с

UserGate серии E является полноценным мощным серверным решением, способным решать задачи по защите от интернет-угроз в сетях с количеством пользователей до тысячи и более.

Для крупных банков и заводов, администраций, ведомственных подразделений, университетов

UserGate F

Модели: F8000



Производительность
межсетевого экрана
до 60 Гб/с

UserGate F8000 сочетает все необходимые функции безопасности с возможностями, необходимыми для функционирования максимально стабильного сервиса при предельно высокой нагрузке.

Для крупных корпоративных сетей, ритейла, дата-центров, университетов, министерств

UserGate X

Модели: X1



Производительность
межсетевого экрана
до 300 Мб/с

Устройство UserGate X1 предназначено для обеспечения комплексной безопасности и информационной защиты критически важных производственных объектов в сложных климатических условиях.

Для промышленных, транспортных объектов на открытом воздухе, банкоматов

Все аппаратные межсетевого экрана UserGate соответствуют требованиям ФСТЭК России, предъявляемым к межсетевым экранам (тип А, Б и Д, 4 класс защиты), системам обнаружения вторжений (уровень узла, 4 класс защиты) и по 4 уровню доверия.



Основные функции

- ✓ Межсетевой экран нового поколения
- ✓ Система обнаружения вторжений (IDS/IPS)
- ✓ Доступ к внутренним ресурсам через SSL VPN Portal Новое
- ✓ Анализ и выгрузка информации об инцидентах безопасности (SIEM) Новое
- ✓ Автоматизация реакции на угрозы безопасности информации (SOAR) Новое
- ✓ Обратный прокси
- ✓ Контроль доступа в интернет
- ✓ Контроль Приложений L7
- ✓ Дешифрование SSL
- ✓ Гостевой портал
- ✓ Безопасная публикация внутренних ресурсов и сервисов
- ✓ Антивирусная защита
- ✓ Advanced Threat Protection
- ✓ Безопасность почты
- ✓ Идентификация пользователей
- ✓ Поддержка концепции BYOD (Bring Your Own Device)
- ✓ Виртуальная частная сеть (VPN)
- ✓ Удаленное администрирование
- ✓ Поддержка АСУ ТП (SCADA)
- ✓ Поддержка кластеризации и высокой отказоустойчивости

Спецификация

Производительность, max	C100	D200	D500	E1000	E3000	F8000	X1
Пропускная способность межсетевого экрана, UDP, Мбит/с	2 000	18 000	20 000	25 000	30 000	60 000	300
Межсетевой экран, трафик EMIX, Мбит/с	2 000	18 000	22 000	27 000	40 000	40 000	70
Межсетевой экран с функцией определения приложений L7, трафик EMIX, Мбит/с	1 910	15 000	18 700	24 000	32 000	40 000	60
Одновременных TCP-сессий	2 000 000	8 000 000	16 000 000	16 000 000	16 000 000	48 000 000	2 000 000
Новых сессий в секунду	10 400	50 000	75 000	100 000	127 000	135 000	5 000
Система обнаружения вторжений, трафик EMIX, Мбит/с	300	1800	2 000	2 800	3 900	8 000	50
Контентная фильтрация, трафик EMIX, Мбит/с	800	8 700	9 500	13 000	14 900	15 000	30
Инспектирование SSL, трафик EMIX, Мбит/с	300	4 000	4 400	5 000	6 500	8 000	10
Контентная фильтрация, антивирус, трафик EMIX, Мбит/с	700	7 900	8 000	12 400	14 900	14 000	20
Межсетевой экран с функцией определения приложений L7, COV, контентная фильтрация, трафик EMIX, Мбит/с	300	1 800	2 000	2 800	3 900	8 000	15
Размер организации							
Рекомендованное количество пользователей	100	300	500	1000	3000	10 000	-
Спецификация оборудования							
Портов 10/100/1000Base-T	5	5 10/1000Base-T 2 SFP 1Gbps + 8 с использованием плат расширений	5 10/1000Base-T 2 SFP 1Gbps + 8 с использованием плат расширений	8 встроено 24 с использованием плат расширений	8 встроено 24 с использованием плат расширений	9 встроено, 40 с использованием плат расширений	2
Портов 10GBase SFP+	-	4 с использованием плат расширений	4 с использованием плат расширений	12 с использованием плат расширений	12 с использованием плат расширений	4 встроено 20 с использованием плат расширений	-
Плат расширений	-	1	1	3	3	3	-
Управление по IPMI*	-	Есть	Есть	Есть	Есть	Есть	-
Процессор, количество ядер	4	8	8	16	28	72	2
Память, Гбайт	8	16	32	32	32	64	8
Диск, Гбайт	1x500	1x1000	1x1000	2x1000, RAID-1	2x1000, RAID-1	2x1000 горячая замена, RAID-1	1x500
Размеры оборудования							
Габариты, мм	Tabletop 230 x 170 x 47.7	1U 438x321x44	1U 438x321x44	1U 438x580x44	1U 438x580x44	2U 438x600x88	57,5x130x127
Вес, кг	1,2	7,5	7,5	16	16	25	1
Крепление в стойку	Кронштейны	Кронштейны	Кронштейны	Комплект рельсов для установки в стойку 19-дюймов	Комплект рельсов для установки в стойку 19-дюймов	Комплект рельсов для установки в стойку 19-дюймов	Монтируемая на DIN-рейку
Электропитание							
Сеть питания, Вольт	140-220	140-220	140-220	140-220	140-220	140-220	12-36
Потребляемая мощность (Макс), Ватт	36	220	220	300	300	800	10.27

* IPMI (Intelligent Platform Management Interface) – интерфейс автономного управления платформой, позволяющий осуществлять управление через командную консоль, а также производить различные сервисные функции, например, создание резервных копий системы, обновление ПО BIOS и т.п. Функции управления платформой могут быть доступны, даже если система находится в выключенном состоянии. **Не предусмотрено для сертифицированной версии.**

Виртуальный межсетевой экран

Модели: VE 100 | VE 250 | VE 500 | VE 1000 | VE 2000 | VE 4000 | VE 6000



UserGate Virtual Edition позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ создан в формате OVF (Open Virtualization Format).

Виртуальная платформа обладает теми же функциями, что и аппаратные устройства UserGate.

Для организаций, которые предпочитают использовать виртуальную инфраструктуру



Быстрое время развертывания

Использование виртуальной инфраструктуры позволяет обеспечить высокую мобильность и гибкость. Виртуальный образ может быть развернут в самое короткое время, это может быть важным как для первоначальной установки, так и для восстановления системы после возникновения нештатной ситуации.

Экономия на аппаратной части

Виртуальные решения работают на уже существующей инфраструктуре заказчика. При этом не возникает необходимость закупки и поддержки нового дорогостоящего сетевого оборудования, а также значительно снижаются риски, связанные с внезапным выходом из строя каких-либо компонентов.

Возможность масштабирования без замены аппаратных платформ

Расширение используемых ресурсов или добавление новых виртуальных машин позволяет быстро обеспечить масштабирование.

Удобство настройки и управления политиками безопасности

Использование эталонного виртуального образа дает возможность обеспечить оперативную установку интернет-шлюзов с определенными настройками безопасности.

Основные функции

- ✓ Межсетевой экран нового поколения
- ✓ Система обнаружения вторжений (IDS/IPS)
- ✓ Доступ к внутренним ресурсам через SSL VPN Portal Новое
- ✓ Анализ и выгрузка информации об инцидентах безопасности (SIEM) Новое
- ✓ Автоматизация реакции на угрозы безопасности информации (SOAR) Новое
- ✓ Обратный прокси
- ✓ Контроль доступа в интернет
- ✓ Контроль Приложений L7
- ✓ Дешифрование SSL
- ✓ Гостевой портал
- ✓ Безопасная публикация внутренних ресурсов и сервисов
- ✓ Антивирусная защита
- ✓ Advanced Threat Protection
- ✓ Безопасность почты
- ✓ Идентификация пользователей
- ✓ Поддержка концепции BYOD (Bring Your Own Device)
- ✓ Виртуальная частная сеть (VPN)
- ✓ Удаленное администрирование
- ✓ Поддержка АСУ ТП (SCADA)
- ✓ Поддержка кластеризации и высокой отказоустойчивости

Спецификация

Производительность	VE 100	VE 250	VE 500	VE 1000	VE 2000	VE 4000	VE 6000
Пропускная способность межсетевого экрана, UDP (Мбит/с)	800	8 000	9 000	10 000	11 000	11 500	12 000
Одновременных TCP сессий	2 000 000	2 000 000	5 000 000	8 000 000	16 000 000	20 000 000	24 000 000
Новых сессий в секунду	24 000	100 000	120 000	130 000	150 000	155 000	160 000
Инспектирование SSL (Мбит/с)	50	300	320	350	600	650	700
Система обнаружения вторжений (IPS), (Мбит/с)	600	1 300	1 350	1 400	1 800	2 100	2 400
Система обнаружения вторжений (IDS), снап-порт, (Мбит/с)	800	1 700	2 000	2 500	3 000	3 200	3 400
Управление приложениями L7, (Мбит/с)	700	1 500	1 700	1 800	2 500	2 800	3 100
Потоковый антивирус, (Мбит/с)	150	1 300	1 500	1 800	2 500	2 800	3 100
Контентная фильтрация, (Мбит/с)	150	1 300	1 500	1 800	2 500	2 800	3 100
Размер организации							
Рекомендованное количество пользователей	100	250	500	1000	2000	4000	6000
Требования к оборудованию							
Портов 10/100/1000Base-T	До 8	До 8	До 8	До 8	До 8	До 8	До 8
Портов 10GBase SFP+	До 8 при использовании вирт. адаптеров VMXNET3						
Процессор, количество ядер	2	4	6	8	16	24	до 32
Память, Гбайт	8	8	16	16	32	32	64
Диск, Гбайт	100	300	300	300	300	300	500

Дополнительные модули и Security Updates

Модуль ATP (Advanced Threat Protection)

- глубокий анализ контента (DCI)
- фильтрация по категориям
- подписка на списки Роскомнадзора и Министерства Юстиции РФ
- черные и белые списки
- подписка на морфологические базы
- автоматическое обновление подписок
- блокировка рекламы (AdBlock)
- контроль за социальными сетями

Модуль Stream Antivirus

- потоковый антивирус UserGate

Модуль Mail Security

- антиспам
- антивирусная проверка почты
- поддержка методов фильтрации спама

Продление дополнительных модулей возможно только при активной подписке на модуль Security Updates.

Модуль Security Updates (SU)

- обновление ПО UserGate
- подписка на обновления баз IPS (сигнатуры атак)
- подписка на обновления баз L7 (сигнатуры приложений)
- стандартный пакет технической поддержки

Подписка на модуль Security Updates сроком на один год включена в базовую лицензию на UserGate. По истечению первого года обязательно ее продление.

Виртуальная платформа UserGate Log Analyzer VE

Модели: VE 6 | VE 14 | VE 25



UserGate Log Analyzer Virtual Edition позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ создан в формате OVF (Open Virtualization Format).

Для организаций, которые предпочитают использовать виртуальную инфраструктуру

Спецификация	VE 6	VE 14	VE 25
Объем хранилища, Тбайт	6	14	25
Количество пользователей	3 000	5 000	10 000

Аппаратная платформа UserGate Log Analyzer F25

Модели: F25



UserGate Log Analyzer F25 предназначен для использования в крупных компаниях и дата-центрах. Данный программно-аппаратный комплекс обладает большими возможностями по хранению информации и обеспечивает максимально быструю обработку данных, получаемых от серверов UserGate.

Для крупных корпоративных сетей, ритейла, дата-центров, университетов, министерств

Спецификация	F 25
Объем хранилища, Тбайт	25
Количество пользователей	10 000

Аппаратная платформа UserGate Log Analyzer E6, E14

Модели: E6 | E14



UserGate Log Analyzer E дополняет функциональность серверного решения UserGate и предназначен для агрегации данных, связанных с анализом инцидентов безопасности, а также для осуществления мониторинга событий и создания отчетов.

Для крупных банков и заводов, администраций, ведомственных подразделений, университетов

Спецификация	E 6	E 14
Объем хранилища, Тбайт	6	14
Количество пользователей	3 000	5 000

Основные функции

- ✓ Уменьшение нагрузки на шлюзы UserGate
- ✓ Обработка журналов и создание отчетов
- ✓ Объединение журналов с нескольких шлюзов для общего анализа
- ✓ Увеличение глубины журналирования
- ✓ Увеличение размера хранилища на серверах LogAn
- ✓ Сбор и анализ информации со сторонних устройств

Виртуальная платформа UserGate Management Center



UserGate Management Center может быть развернут на виртуальной инфраструктуре заказчика.

Виртуальная машина поставляется с двумя Ethernet-интерфейсами.

Для организаций, которые предпочитают использовать виртуальную инфраструктуру

Спецификация	VE
Количество управляемых устройств	Зависит от конфигурации

Аппаратная платформа UserGate Management Center E



UserGate Management Center E поддерживает управление и поддержку распределенного парка межсетевых экранов UserGate для средних и крупных организаций с филиальной сетью.

Данное устройство поставляется с уже загруженным и готовым к первоначальной настройке программным обеспечением.

Для интернет-провайдеров и больших корпоративных сетей

Спецификация	E
Количество управляемых устройств	До 1000

Аппаратная платформа UserGate Management Center C



UserGate Management Center C поддерживает управление и поддержку двух и более межсетевых экранов для небольших организаций и их филиалов.

Данное устройство поставляется с уже загруженным и готовым к первоначальной настройке программным обеспечением.

Для малого бизнеса, филиалов, POS-систем, Wi-Fi-точек, школ

Спецификация	C
Количество управляемых устройств	До 50

Основные функции

- ✓ Единый сервер управления
- ✓ Поддержка облачной платформы управления
- ✓ Применение общих политик и настроек
- ✓ Поддержка распределенного парка межсетевых экранов
- ✓ Создание управляемых областей
- ✓ Управление кластерами



ООО «Юзергейт»

Телефон: **8 (800) 500 4032**

Клиентам: sales@usergate.com

Партнерам: partner@usergate.com

121087, г. Москва,
Береговой проезд, 5А, к.1, 21 этаж

630090, г. Новосибирск, Центр
Информационных Технологий, Технопарк
Академгородка,
ул. Николаева, 11, этаж 6

680021, г. Хабаровск,
ул. Ленинградская, 46, офис 2



SC Awards
finalist



Лучшие IT-решения
для повышения эффективности
**ЦИФРОВЫЕ
ВЕРШИНЫ**

SC Awards
finalist

Sk
ИТ