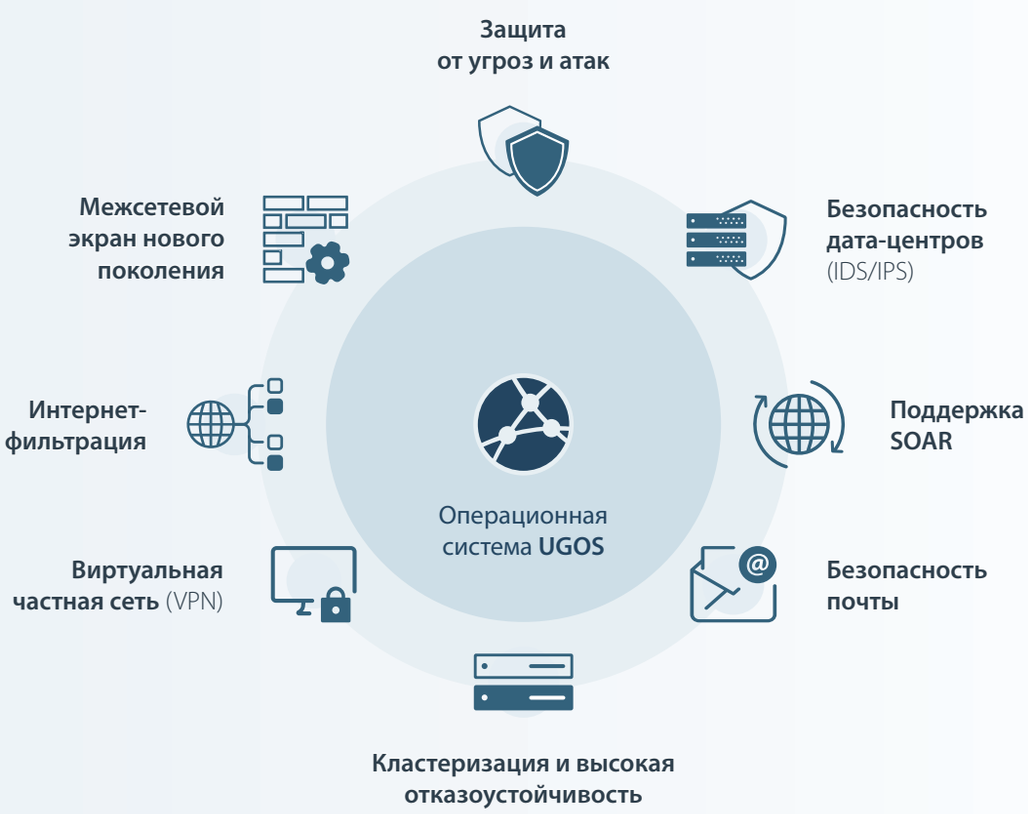
UserGate

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 законам РФ

- UserGate соответствует требованиям ФСТЭК России к профилям защиты межсетевых экранов типа А и Б 4 класса защиты, системам обнаружения вторжений 4 класса защиты и по 4 уровню доверия
- UserGate внесен в Реестр Российского программного обеспечения (регистрационный номер 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.

UserGate

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.

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 (Internet filtering)

Использование интернет-фильтрации значительно увеличивает безопасность локальной сети, так как позволяет обеспечить административный контроль за использованием интернета, закачками, 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.

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 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.

Функции

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.

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.

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.

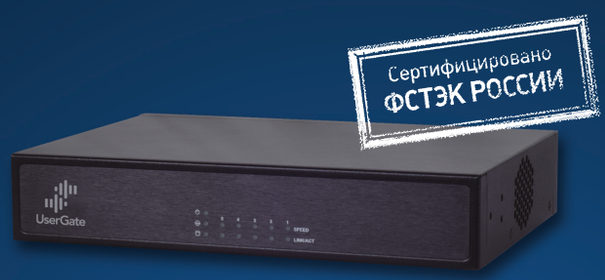
В решении реализована поддержка кластеризации в режиме active-active и active-passive. Кластеризация позволяет применять к разным нодам единые настройки, политики, библиотеки, сертификаты, сервера авторизации, группы пользователей и т. д.

Межсетевой экран C100

Для небольших предприятий, филиалов, POS-систем, образования

Сети любого размера должны быть защищены от внешних атак, вирусов и разнообразных современных киберугроз.

UserGate C100 является компактным и удобным в настройке сетевым устройством, обеспечивающим безопасность сетей небольших организаций или филиалов.



Доступность и удобство

UserGate C100 предлагается по минимальным ценам, что делает его доступным для небольших организаций, а также для использования в филиалах, таких, как точки продаж.

Устройство поставляется практически готовым к использованию, и его настройка может быть произведена обычным системным администратором. UserGate C100 может использоваться в сетях с шириной канала пропускания до 2 Гб/с.

Комплексная безопасность

Несмотря на компактность и невысокую стоимость модели UserGate C100, работа устройства основана на тех же технологиях, которые используются и для защиты сетей крупных компаний.

С его помощью можно обеспечить не только базовую функциональность межсетевого экранирования, но и защиту от современных атак, анализ и фильтрацию трафика по контенту, контроль интернет-приложений, блокирование опасных скриптов и приложений, защиту от Dos-атак, вирусов и спама, а также другие функции безопасности.

Кроме этого UserGate C100 может обеспечить защиту гостевого Wi-Fi и дает возможность контроля персональных устройств, таких, как смартфоны и планшет (концепция BYOD - Bring Your Own Device).

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	
Пропускная способность межсетевого экрана, UDP (Мбит/с)	**2 000**
Одновременных TCP сессий	**2 000 000**
Новых сессий в секунду	**34 000**
Инспектирование SSL (Мбит/с)	**70**
Система обнаружения вторжений (IPS), (Мбит/с)	**800**
Система обнаружения вторжений (IDS), span-порт, (Мбит/с)	**1 000**
Управление приложениями L7, (Мбит/с)	**850**
Потоковый антивирус, (Мбит/с)	**200**
Контентная фильтрация, (Мбит/с)	**200**

Размер организации	
Рекомендованное количество пользователей	**100**

Спецификация оборудования	
Портов 10/100/1000Base-T	**5**
Процессор, количество ядер	**4**
Память, Гбайт	**8**
Диск, Гбайт	**1x500**

Размеры	
Габариты, мм	**Tabletop** **230 x 170 x 47.7**
Вес, кг	**1,2**
Крепление в стойку	**Кронштейны**

Электропитание	
Сеть питания, Вольт	**140-220**
Потребляемая мощность (Макс), Ватт	**36**

Дополнительные модули и подписка 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
- потоковый антивирус
- блокировка рекламы (AdBlock)
- контроль за социальными сетями

Антивирусный модуль с эвристическим анализом

Модуль Mail Security:

- антиспам
- потоковый антивирус
- 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

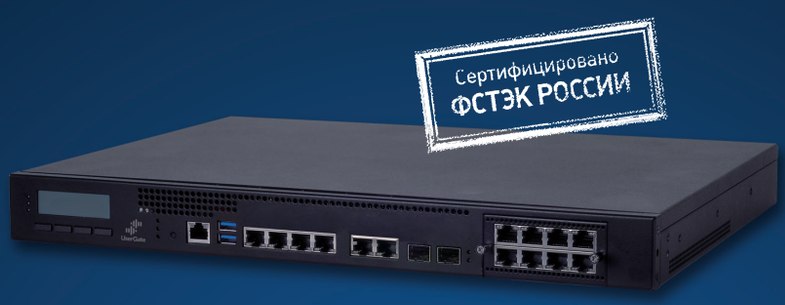
Подписка на модуль Security Updates сроком на один год включена в базовую лицензию на UserGate. По истечению первого года обязательно ее продление.

Межсетевой экран D200, D500

Для предприятий среднего размера, ритейла, образования и филиалов

Для защиты корпоративных сетей необходимо использовать многофункциональное решение, способное обеспечить комплексную безопасность сетевой инфраструктуры без негативного влияния на скорость доступа.

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



Защита от интернет-угроз

Любая сетевая инфраструктура, особенно подключенная к интернету, подвержена опасным внешним воздействиям. UserGate D обеспечивает надежную защиту от современных атак, анализ и фильтрацию трафика по контенту, контроль интернет-приложений, блокирование опасных скриптов и приложений, защиту от DoS-атак, вирусов и спама, а также другие функции безопасности.

Контроль пользователей и сетевого трафика

Безопасность корпоративных сетей не может быть обеспечена без надлежащего контроля за деятельностью пользователей, при этом важность этого контроля напрямую зависит от размера сети. UserGate D обеспечивает соблюдение корпоративных политик для групп пользователей, а также предоставляет защиту гостевого Wi-Fi, дает возможность контроля персональных устройств, таких, как смартфоны и планшет (концепция BYOD – Bring Your Own Device).

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	D200	D500
Пропускная способность межсетевого экрана, UDP (Мбит/с)	18 000	20 000
Одновременных TCP сессий	8 000 000	16 000 000
Новых сессий в секунду	145 000	160 000
Инспектирование SSL (Мбит/с)	400	750
Система обнаружения вторжений (IPS), (Мбит/с)	1 600	2 000
Система обнаружения вторжений (IDS), span-порт, (Мбит/с)	2 000	3 000
Управление приложениями L7, (Мбит/с)	1 700	2 100
Потоковый антивирус, (Мбит/с)	1 500	2 000
Контентная фильтрация, (Мбит/с)	1 500	2 000

Размер организации		
Рекомендованное количество пользователей	300	500

Спецификация оборудования		
Портов 10/100/1000Base-T	5 10/100/1000Base-T 2 SFP 1Gbps + 8 с использованием плат расширений	5 10/100/1000Base-T 2 SFP 1Gbps + 8 с использованием плат расширений
Портов 10GBase SFP+	4 с использованием плат расширений	4 с использованием плат расширений
Плат расширений	1	1
Управление по IPMI*	Есть	Есть
Процессор, количество ядер	8	8
Память, Гбайт	16	32
Диск, Гбайт	1x1000	1x1000

Размеры		
Габариты, мм	1U 438x321x44	1U 438x321x44
Вес, кг	7,5	7,5
Крепление в стойку	Кронштейны	Кронштейны

Электропитание		
Сеть питания, Вольт	140-220	140-220
Потребляемая мощность (Макс), Ватт	220	220

* 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.

Межсетевой экран E1000, E3000

Для больших корпоративных сетей

Для больших корпоративных сетей необходимо использование высокопроизводительной платформы, имеющей запас прочности и возможности по масштабированию.

UserGate E является мощным сетевым серверным решением, способным решать задачи по защите от всевозможных интернет-угроз, а также осуществлять дешифрацию и глубокий анализ трафика в сетях с несколькими тысячами пользователей.

Комплексная защита инфраструктуры

Для средних и крупных предприятий крайне важно использование надежных и производительных систем безопасности. UserGate E эффективно защищает корпоративную сеть от современных атак и других вторжений, обеспечивает анализ и фильтрацию трафика по контенту, контроль интернет-приложений, блокирование опасных скриптов и приложений, защиту от вирусов и спама, а также другие функции безопасности.

Контроль пользователей и сетевого трафика

Средним и крупным предприятиям необходимо обеспечение безопасности как корпоративной инфраструктуры, так и соблюдение корпоративных политик. UserGate E поддерживает большое количество способов авторизации пользователей, позволяет применять индивидуальные политики безопасности для различных групп, отслеживать и контролировать действия как корпоративных, так и гостевых пользователей.

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	E1000	E3000
Пропускная способность межсетевого экрана, UDP (Мбит/с)	25 000	30 000
Одновременных TCP сессий	16 000 000	16 000 000
Новых сессий в секунду	170 000	182 000
Инспектирование SSL (Мбит/с)	1 000	1 300
Система обнаружения вторжений (IPS), (Мбит/с)	2 800	3 900
Система обнаружения вторжений (IDS), span-порт, (Мбит/с)	3 900	4 800
Управление приложениями L7, (Мбит/с)	2 800	3 900
Потоковый антивирус, (Мбит/с)	2 300	3 300
Контентная фильтрация, (Мбит/с)	2 300	3 300

Размер организации		
Рекомендованное количество пользователей	1 000	3 000

Спецификация оборудования		
Портов 10/100/1000Base-T	8 встроено 24 с использованием плат расширений	8 встроено 24 с использованием плат расширений
Портов 10GBase SFP+	12 с использованием плат расширений	12 с использованием плат расширений
Плат расширений	3	3
Управление по IPMI	Есть	Есть
Процессор, количество ядер	16	28
Память, Гбайт	32	32
Диск, Гбайт	2x1000, RAID-1	2x1000, RAID-1

Размеры оборудования		
Габариты, мм	1U 438x580x44	1U 438x580x44
Вес, кг	16	16
Крепление в стойку	Комплект рельс для установки в стойку 19-дюймов	Комплект рельс для установки в стойку 19-дюймов

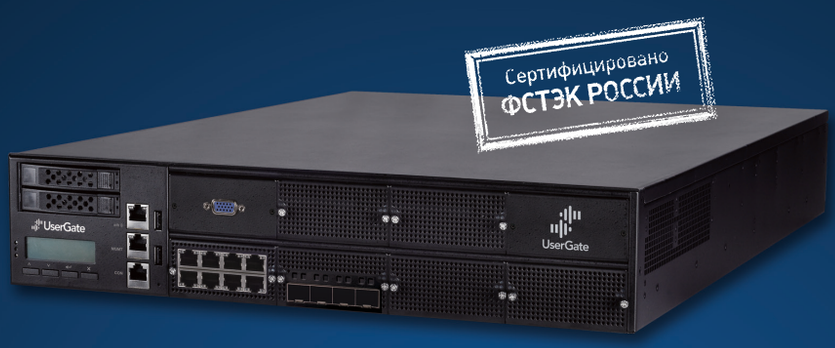
Электропитание		
Сеть питания, Вольт	140-220	140-220
Потребляемая мощность (Макс), Ватт	300	300

Межсетевой экран F8000

Для крупных корпоративных сетей и дата-центров

Для крупных корпоративных сетей и дата-центров критично использование надежных сетевых решений, обеспечивающих высокую доступность, резервирование, масштабируемость и гибкость относительно встраивания в сетевую инфраструктуру.

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



Комплексная защита инфраструктуры

Крупные проекты выдвигают особые требования к производительности, безопасности и отказоустойчивости сети.

UserGate F8000 работает на базе максимально мощных платформы и процессоров, обеспечивая высокую производительность сети за счет кластеризации (VRRP), возможности создания бондов и мостов, динамической маршрутизации (OSPF, BGP) балансировки нагрузки, а также использования VPN для объединения разрозненных офисов в единую логическую сеть.

Контроль абонентов и пользователей

Корпоративный межсетевой экран UserGate F8000 обеспечивает безопасность и соблюдение корпоративных политик для предприятий любого размера и может использоваться в операторских проектах и для предоставления облачных сервисов.

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	F8000
Пропускная способность межсетевого экрана, UDP (Мбит/с)	57 000
Одновременных TCP сессий	48 000 000
Новых сессий в секунду	448 500
Инспектирование SSL (Мбит/с)	2 000
Система обнаружения вторжений (IPS), (Мбит/с)	8 000
Система обнаружения вторжений (IDS), span-порт, (Мбит/с)	14 000
Управление приложениями L7, (Мбит/с)	8 000
Потоковый антивирус, (Мбит/с)	4 000
Контентная фильтрация, (Мбит/с)	4 000

Размер организации	
Рекомендованное количество пользователей	10 000

Спецификация оборудования	
Портов 10/100/1000Base-T	9 встроено 40 с использованием плат расширений
Портов 10GBase SFP+	4 встроено 20 с использованием плат расширений
Плат расширений	3
Управление по IPMI	Есть
Процессор, количество ядер	72
Память, Гбайт	64
Диск, Гбайт	2x1000, горячая замена, RAID-1

Размеры оборудования	
Габариты, мм	2U 438x600x88
Вес, кг	25
Крепление в стойку	Комплект рельс для установки в стойку 19-дюймов

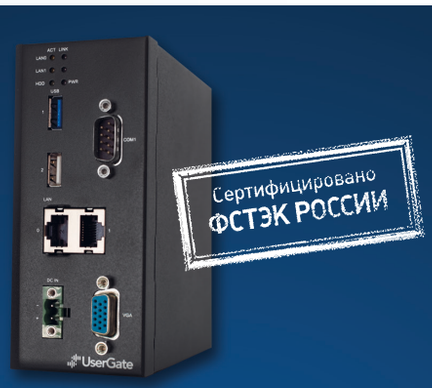
Электропитание	
Сеть питания, Вольт	140-220
Потребляемая мощность (Макс), Ватт	800

UserGate

Межсетевой экран X1

Промышленные, транспортные объекты на открытом воздухе

В современном мире к интернету и различным сетям подключены не только офисные компьютеры, но и многочисленные устройства, управляющие уличной, транспортной, промышленной и другими инфраструктурами. Безопасность таких объектов крайне важна, но ее не всегда можно обеспечить стандартными средствами в силу экстремальных условий эксплуатации.



Работа в экстремальных условиях

UserGate X, в отличие от других устройств, рассчитан на работу в самых суровых условиях: при температурах от -40C^0 до +70C^0 и относительной влажности от 5% до 95%. Модель имеет компактный размер, вес около 1 кг и настенное крепление или крепление на DIN-рейку.

Все это делает возможным ее применение для защиты промышленных, транспортных и других объектов, расположенных на открытом воздухе.

Комплексная безопасность

Работа модели UserGate X основана на тех же технологиях, что используются в решениях UserGate для защиты корпоративных сетей. С ее помощью можно обеспечить функциональность межсетевого экрана (NGFW – Next Generation Firewall), защиту от атак (IDPS – Intrusion Detection and Prevention System), блокирование опасных скриптов и приложений, защиту от вирусов, а также другие функции безопасности. Устройство обрабатывает трафик со скоростью до 300 Мб/с в режиме межсетевого экрана и до 10-15 Мб/с в режиме с включенными функциями безопасности (предотвращение вторжений, защита от угроз и т.д).

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	X1
Пропускная способность межсетевого экрана, UDP (Мбит/с)	**800**
Одновременных TCP сессий	**2 000 000**
Новых сессий в секунду	**10 000**
Инспектирование SSL (Мбит/с)	**10**
Система обнаружения вторжений (IPS), (Мбит/с)	**50**
Система обнаружения вторжений (IDS), span-порт, (Мбит/с)	**70**
Управление приложениями L7, (Мбит/с)	**60**
Потоковый антивирус, (Мбит/с)	**15**
Контентная фильтрация, (Мбит/с)	**15**

Спецификация оборудования	
Портов 10/100/1000Base-T	**2**
Процессор, количество ядер	**2**
Память, Гбайт	**8**
Диск, Гбайт	**1x500**

Размеры оборудования	
Габариты, мм	**57,5x130x127**
Вес, кг	**1**
Крепление в стойку	**Монтируемая на DIN-рейку**

Электропитание	
Сеть питания, Вольт	**12-36**
Потребляемая мощность (Макс), Ватт	**10.27**

UserGate

Виртуальный межсетевой экран UserGate

UserGate может быть развернут на виртуальной инфраструктуре заказчика. При этом поддерживается работа с любыми гипервизорами, такими как VMware, Hyper-V, Xen, KVM, OpensStack, VirtualBox.

Функциональность виртуального решения полностью эквивалентна той, что предоставляется аппаратными комплексами UserGate.

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

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 аппаратную часть

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), span-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

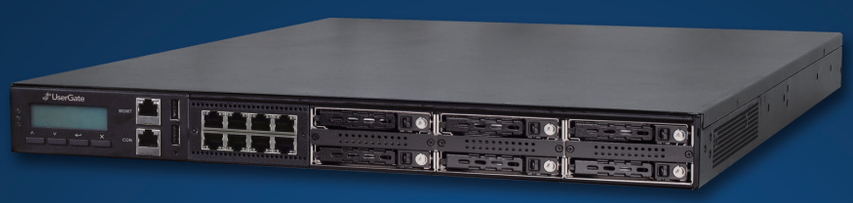
Требования к оборудованию							
Портов 10/100/1000Base-T	До 8	До 8	До 8	До 8	До 8	До 8	До 8
Портов 10GBase SFP+	до 8 при использовании вирт. адаптеров VMXNET3						
Процессор, количество ядер	2	4	6	8	16	24	до 32
Память, Гбайт	8	8	16	16	32	32	64
Диск, Гбайт	100	300	300	300	300	300	500

UserGate Log Analyzer E6, E14

Для больших корпоративных сетей

UserGate Log Analyzer осуществляет сбор и первичную обработку данных от межсетевых экранов UserGate.

Продукт развертывается отдельно от шлюза безопасности UserGate и является полноценным сетевым серверным решением, способным решать задачи по защите от всевозможных интернет-угроз в сетях с количеством пользователей до тысячи и более.



Комплексная защита инфраструктуры

Для средних и крупных предприятий крайне важно использование надежных и производительных систем безопасности. 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.

Отчеты

На основании полученных данных UserGate Log Analyzer осуществляет глубокий анализ произошедших событий безопасности, определяет и отслеживает подозрительные активности отдельных пользователей или хостов, что в том числе необходимо для соответствия современной концепции SOAR (Security Automation, Orchestration and Response).

Настраивая UserGate, можно указать какие типы событий пересылаются для анализа в Log Analyzer:

- Журнал событий;
- Журнал системы обнаружения вторжений;
- Журнал трафика, события АСУ ТП;
- События из журнала веб-доступа.

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

Спецификация

Производительность	E6	E14
Расчетное время хранения журналов, дней	**1 020**	**1 428**

Размер организации		
Рекомендованное количество пользователей	**3 000**	**5 000**

Спецификация оборудования		
Портов 10/100/1000Base-T	**8 встроено**	**8 встроено**
Процессор, количество ядер	**8**	**8**
Объем хранилища, Тбайт	**6, RAID-5 с горячим резервом**	**14, RAID-5 с горячим резервом**

Размеры оборудования		
Габариты, мм	**1U 438x580x44**	**1U 438x580x44**
Вес, кг	**16**	**16**
Крепление в стойку	**Комплект рельс для установки в стойку 19-дюймов**	**Комплект рельс для установки в стойку 19-дюймов**

Электропитание		
Сеть питания, Вольт	**140-220**	**140-220**
Потребляемая мощность (Макс), Ватт	**300**	**300**

UserGate Log Analyzer F25

Для крупных корпоративных сетей и дата-центров

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.

Комплексная защита инфраструктуры

Крупные проекты накладывают особые требования на производительность системы. UserGate Log Analyzer F25 дополняет функциональность серверного решения UserGate, работает на базе максимально мощных платформы и процессоров и предназначен для агрегации данных, связанных с анализом инцидентов безопасности, а также для осуществления мониторинга событий и создания отчетов.

Отчеты

На основании полученных данных UserGate Log Analyzer осуществляет глубокий анализ произошедших событий безопасности, определяет и отслеживает подозрительные активности отдельных пользователей или хостов, что в том числе необходимо для соответствия современной концепции SOAR (Security Automation, Orchestration and Response).

Настраивая UserGate, можно указать какие типы событий пересылаются для анализа в Log Analyzer:

- Журнал событий;
- Журнал системы обнаружения вторжений;
- Журнал трафика, события АСУ ТП;
- События из журнала веб-доступа.

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

Спецификация

Производительность	F25
Расчетное время хранения журналов, дней	**1 275**

Размер организации	
Рекомендованное количество пользователей	**10 000**

Спецификация оборудования	
Портов 10/100/1000Base-T	**9 встроено**
Процессор, количество ядер	**32**
Объем хранилища, Тбайт	**25, RAID-5 с горячим резервом**

Размеры оборудования	
Габариты, мм	**2U 438x600x88**
Вес, кг	**25**
Крепление в стойку	**Комплект рельс для установки в стойку 19-дюймов**

Электропитание	
Сеть питания, Вольт	**140-220**
Потребляемая мощность (Макс), Ватт	**800**

Виртуальная платформа UserGate Log Analyzer

UserGate Log Analyzer может быть развернут на виртуальной инфраструктуре заказчика. При этом поддерживается работа с любыми гипервизорами, такими как VMware, Hyper-V, Xen, KVM, OpensStack, VirtualBox.

Функциональность виртуального решения полностью эквивалентна той, что предоставляется аппаратной комплексами UserGate Log Analyzer.

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

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 аппаратную часть

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

- ✓ 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

Спецификация

Производительность	VE 6	VE 14	VE 25
Расчетное время хранения журналов, дней	**1 020**	**1 428**	**1 275**

Размер организации			
Рекомендованное количество пользователей	**3 000**	**5 000**	**10 000**

Требования к оборудованию			
Процессор, количество ядер	**От 10**	**От 12**	**От 32**
Память, Гбайт	**От 32**	**От 32**	**От 64**
Объем хранилища, Тбайт	**От 6**	**От 14**	**От 35**

UserGate

ООО «Юзергейт»

Телефон: **8 (800) 500 4032**

Клиентам: sales@usergate.com

Партнерам: partner@usergate.com

121205, г. Москва, территория
Инновационного центра «Сколково»,
ул. Нобеля, 7, этаж 4

630090, г. Новосибирск, Центр
Информационных Технологий, Технопарк
Академгородка,
ул. Николаева, 11, офис 602

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

SC Magazine Awards 2014 Finalist Honored in the U.S.

SC Magazine Awards 2015 Europe Winner

2015 Computing Security Awards ★ Finalist ★

SC 2017 Awards finalist

Лучшие IT-решения для повышения эффективности ЦИФРОВЫЕ ВЕРШИНЫ

SC 2020 Awards finalist