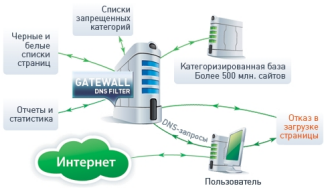
**GateWall DNS Filter** позволяет обеспечить максимальный контроль использования Интернета без использования программных и аппаратных прокси-серверов и интернет-шлюзов в вашей сети. Работа продукта основана на фильтрации DNS запросов. Использование GateWall DNS Filter увеличивает безопасность Интернета, уменьшает нецелевой трафик и улучшает продуктивность работы пользователей Интернета.

Работа GateWall DNS Filter основана на технологии Entensys URL Filtering 2.0, которая также используется в UserGate Proxy & Firewall и KinderGate Родительский Контроль.




## Блокировка категорий сайтов

GateWall DNS Filter использует крупнейшую базу из 500 миллионов категоризированных сайтов. Администратор может легко настроить блокировку сайтов, относящихся к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети, торренты и пиринговые сети, прокси-сервера, анонимайзеры и другие. Возможно также создание белых списков, обеспечивающих гарантированный доступ к определенным сайтам или же, наоборот, блокировка определенных сайтов, не зависящая от прочих настроек.

Администрирование программного решения осуществляется через веб-интерфейс. Решение позволяет устанавливать настройки разных групп. Это дает возможность использовать один сервер для большого числа клиентов, каждый из которых может

самостоятельно и независимо управлять настройками фильтрации и иметь доступ к статистике своих пользователей.

---

**Безопасность доступа в Интернет**

GateWall DNS Filter обеспечивает блокировку сайтов, связанных с фишингом, троянами, кейлогерами, ботнетами и других сайтов, содержащими вредоносные программы.

**Опасности, связанные с использованием Интернета**

Интернет становится все более и более опасной средой. Существуют миллионы сайтов, содержащих вредоносные программы, тройаны, кейлоггеры и прочие опасности. В последнее время появились новые опасности, связанные с рапространением социальных сетей. Злоумышленники стали больше использовать личную информацию и схемы мошеничества стали более изощренными.

К сожалению, использование антивирусов и прочих средств интернет-безопасности на рабочих станциях не всегда решает данную проблему. Пользователи не всегда правильно используют данные средства, возможно их отключение, несвоевременное обновление и т.д.

**Динамический подход**

В технологии Entensys URL Filtering используется динамический подход к категоризации сайтов и выявлению опасных ресурсов. Статический подход подразумевает, что однажды категоризированный сайт остается в этой категории на неопределенное время. В случае динамического подхода производится постоянный мониторинг всех сайтов. В результате этого выявляются ресурсы, содержание которых изменилось и они проходят повторную категоризацию.

В базе, используемой Entensys URL Filtering, ежедневно обновляются около 100 000 сайтов.

---

**Отчеты и мониторинг**

GateWall DNS Filter предоставляет возможность получать статистику по посещенным категориям сайтов, по разрешенным и блокированным хитам. Использование данных отчетов позволяет качественно анализировать проблемы, связанные с нецелевым использованием Интернета.

---

**«Облачная» модель**

GateWall DNS Filter может устанавливаться на один из локальных серверов, тогда пользователь сам настраивает сервер и контролирует его работу.

Другой вариант - это использование GateWall DNS Filter Cloud. В этом случае необходимо лишь подписаться на использование данного сервиса и перенастроить адреса локальных DNS серверов.

GateWall DNS Filter также упакован по открытому стандарту APS, что обеспечивает возможность удобного развертывания в «облаке» и встраивания в системы различных

сервис-провайдеров.

В любом случае использование GateWall DNS Filter не требует установки и настройки локальных аппаратных и программных комплексов. Сохраняется текущая топология сети, настройки безопасности и работа всех существующих приложений. Обновление базы сайтов происходит незаметно для пользователя и не влияет на его работу.

---

**Text Filtering**

В продукт внедрен специальный модуль **Text Filtering**, который позволяет выполнять морфологический анализ страниц, загружаемых пользователем, посредством словаря, заданного администратором.

С появлением новой системы GateWall DNS Filter приобрел также достаточные для внедрения в высоконагруженные сети интернет-провайдеров показатели отказоустойчивости и возможности масштабирования. Интеграция продукта с Text Filtering в личный кабинет оператора осуществляется с помощью специально разработанного API. Для внедрения необходимо использовать прокси-сервер на базе OS Linux, поддерживающий работу ICAP (Internet Content Adaptation Control).

---

**Сфера использования**

**Школы и образовательные учреждения**

Подключение школ к Интернету является одним из приоритетов нац. проекта «Образование». Осуществление контроля за Интернетом в школах просто необходимо. Технически это осуществимо либо через контроль на уровне шлюза с помощью прокси-сервера, например, UserGate Proxy & Firewall, либо через фильтрацию DNS

запросов. Преимуществом DNS-фильтра является легкость в установке и его централизованная настройка на уровне города или региона. Такой подход позволяет обеспечивать контроль Интернета и в удаленных сельских школах, где не всегда возможна полноценная настройка интернет-шлюза.

**Другие государственные учреждения**

С каждым годом государство внедряет проекты, основанные на технологиях тесно связанных с Интернетом. Поэтому возникает вопрос безопасности и контроля его использования. GateWall DNS Filter может использоваться в организациях социального страхования, налоговых инспекциях, администрациях городов, областей.

**Средние и крупные компании**

Использование DNS-фильтрации является самым простым и доступным решением по обеспечению фильтрации трафика в крупных и средних компаниях. GateWall DNS Filter позволяет в рамках одного проекта обеспечить контроль за большим количеством подразделений или филиалов. В качестве примера можно выделить банки, страховые компании, торговые сети и т.д.

**Интернет-провайдеры**

GateWall DNS Filter может быть внедрен на уровне провайдера (домовые сети, провайдеры второго уровня, крупные провайдеры, бизнес-центры). В этом случае провайдер может предоставлять своим пользователям, как частным, так и корпоративным, дополнительный сервис по фильтрации Интернета. Это может быть востребовано как с позиции родительского контроля, так и с позиции контроля за эффективностью работы сотрудников.

---

**Системные требования**

Физический или виртуальный сервер

OS Windows XP/2003/7/2008/2008 R2

CPU 2 HGz

RAM 1 Gb

HD 2 Gb максимум + файлы кэша HTTP прокси-сервера.