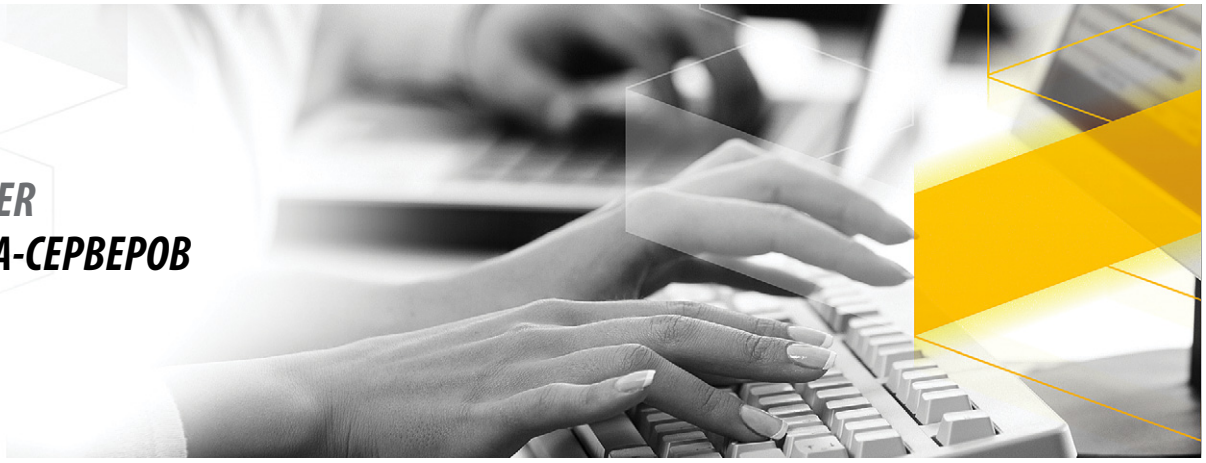


BITDEFENDER
ЗАЩИТА ISA-СЕРВЕРОВ

ИНТЕРНЕТ-ШЛЮЗЫ — ПЕРВАЯ ЛИНИЯ ЗАЩИТЫ

На сегодняшний день организации предоставляют большинству сотрудников совместный доступ к сети Интернет, поэтому веб-службы прокси являются надежным средством управления использованием канала и объединения трафика путем локального кэширования данных. Использование доступа к сети Интернет в личных и служебных целях существенно увеличивает объем Интернет-трафика и, в свою очередь, повышает уязвимость для угроз. Таким образом, решения для защиты Интернет-шлюза предприятия (например, Microsoft® Internet Security and Acceleration (ISA) Server) обеспечивают значительно более быстрое время отклика и повышение функциональности брандмауэра, представляющего собой первую линию защиты.

ПОТРЕБНОСТЬ В ЗАЩИТЕ ШЛЮЗОВ ДОСТУПА В ИНТЕРНЕТ

Хотя дополнительная защита брандмауэром шлюзов доступа в Интернет является бесспорным плюсом, такая защита ограничивается статическими правилами брандмауэра и недостаточной "прозрачностью" пакетов, проходящих через шлюз. Таким образом, защита от проникновения вредоносного кода в локальную сеть предприятия через неотслеживаемые приложения или вследствие недостаточно тщательной проверки содержимого может привести к потере огромного количества времени, денег и ресурсов ИТ-инфраструктуры в случае заражения.

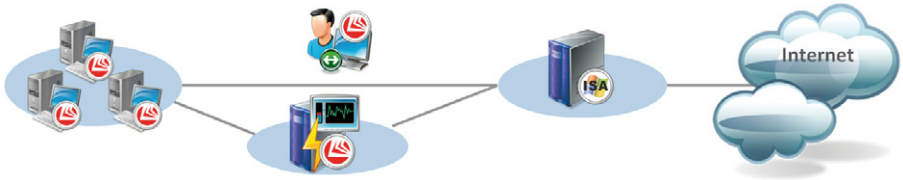
Веб-службы могут представлять угрозу безопасности, например:

- Веб-сайты или загружаемые файлы, инфицированные вредоносным кодом
- Загрузка инфицированных вложений электронной почты из почтовых веб-служб
- Загрузка и отправка инфицированных файлов посредством FTP-служб
- Посредством вирусов, распространяемых через общедоступный сетевой диск

Шлюз является центральным пропускным пунктом для веб-содержимого, что позволяет предприятиям обеспечивать соблюдение пользователями требований политики безопасности в отношении как входящего, так и к исходящего содержимого в рамках сети. В целях оптимизации системы безопасности и повышения устойчивости при развертывании ISA-сервера без влияния на время выполнения и отклика для критических операций требуются дополнительные решения, которые способны обеспечить неизменную эффективность работы.

ЗАЩИТА ИНТЕРНЕТ-ШЛЮЗОВ С ПОМОЩЬЮ РЕШЕНИЙ BITDEFENDER

BitDefender Security for ISA Servers обеспечивает для предприятий защиту серверов Microsoft® ISA Server® путем блокирования веб-сайтов определенных типов, сканирования загружаемых файлов и вложений, загружаемых из веб-служб электронной почты. Это значительно упрощает соблюдение корпоративных политик безопасности, благодаря чему предприятия смогут контролировать критически важную информацию, которая в ином случае была бы подвержена риску утечки из внутренней сети организации.



BitDefender Security for ISA Servers scans inbound and outbound Web and FTP traffic and applies a set of scanning or filtering rules that are configurable through a Centralized Management Server.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ПРЕИМУЩЕСТВА

- ***Знаменитая система распознавания, очистки и карантина вирусов***
- ***Минимизация времени простоя сети в целях повышения эффективности эксплуатации***
- ***Минимизация угроз безопасности, сокращение стоимости ресурсов и накладных расходов, повышение производительности***
- ***Технология оптимизации работы браузера посредством сканирования и разбивки крупных файлов на блоки небольшого размера***
- ***Простые в управлении списки блокируемых веб-сайтов и FTP-серверов с синтаксисом на основе ключевых слов, а также списки разрешенных веб-сайтов***
- ***Сканирование файлового трафика для обеспечения защиты от вредоносного ПО в режиме реального времени и снижения риска распространения вирусов в корпоративной сети***
- ***Интеграция с правилами брандмауэра Microsoft и веб-кэширование посредством антивирусного интерфейса Microsoft (ISAPI) в целях оптимизации и повышения скорости сканирования***
- ***Отчеты об активности вирусов, статистика сканирования и учет интернет-трафика***
- ***Настраиваемые действия для различных событий, вызывающих оповещение по электронной почте или выполнение других действий***
- ***Поддержка больших объемов на нескольких ISA-серверах, настроенных как массивы в целях распределения нагрузки***
- ***Обеспечивает возможность удаленной настройки с любого компьютера в сети предприятия посредством консоли централизованного управления***

Bitdefender

ТЕХНОЛОГИИ BITDEFENDER

Все решения BitDefender используют патентованную технологию B-HAVE, с помощью которой выполняется анализ поведения возможного вредоносного кода в пределах виртуального компьютера, благодаря чему исключаются ложные обнаружения и значительно повышается уровень распознавания новых и неизвестных вредоносных программ.

АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ

BitDefender Security for ISA Servers представляет интеллектуальную систему ежечасного обновления вирусных сигнатур, благодаря чему обеспечивается постоянное соответствие уровня защиты среды Microsoft® ISA Server текущему состоянию угроз.

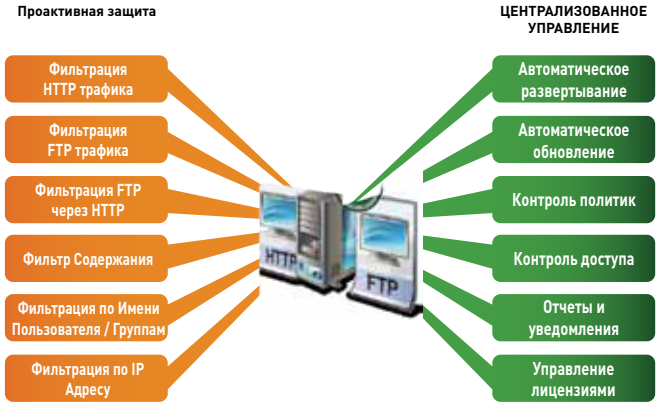
ВСЕСТОРОННЯЯ ЗАЩИТА

BitDefender Security for ISA Servers представляет собой лишь один из компонентов комплексной системы решений, обеспечивающих полную защиту сети от шлюза до рабочей станции. Проактивные многоплатформенные решения BitDefender выполняют обнаружение и предотвращают проникновение вирусов, шпионских и рекламных программ, а также "троянских коней", способных скомпрометировать целостность сети.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Программное обеспечение

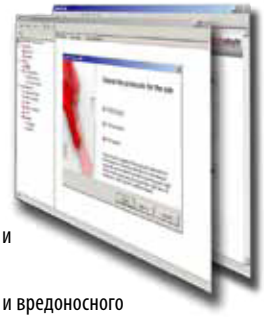
- Windows Server 2003 SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2
- Microsoft ISA Server 2000/2004/2006 Standard Edition
- Microsoft ISA Server 2004/2006 Enterprise Edition
- Internet Explorer 6.0 или более поздней версии



BitDefender Security for ISA Servers является общепризнанным инструментом антивирусной защиты, управления и отчетности, который делает возможным безопасную совместную работу с данными в масштабах всего предприятия

ЕСКОЛЬКО УРОВНЕЙ СКАНИРОВАНИЯ И ФИЛЬТРАЦИИ

Знаменитые системы сканирования BitDefender признаны ведущими органами сертификации, включая ICSA Labs, Virus Bulletin и West Coast Labs, благодаря не имеющей аналогов профилактической защите от вредоносного ПО. Решения BitDefender используют методологию сканирования и фильтрации на нескольких уровнях, позволяющую распознавать вредоносный код и обеспечить надежную защиту конфиденциальной информации;



Веб-трафика (HTTP-трафика) обеспечивает распознавание вирусов и вредоносного ПО в режиме реального времени при посещении пользователями веб-сайтов, использовании веб-служб электронной почты и других веб-приложений.

загрузки и отправки по протоколу FTPобеспечивают обнаружение вирусов и вредоносного ПО в режиме реального времени при каждой загрузке или отправке пользователем файлов с использованием протокола передачи файлов (FTP).

Фильтрация содержимого — фильтрация содержимого позволяет распознавать определенную информацию (данные кредитных карт и счетов, наименования отчетов, базы данных клиентов и пр.) и предотвратить выход таких сведений из-под контроля предприятия. Фильтрация содержимого представляет собой настраиваемые ограничения на основе адресов веб-сайтов или FTP-серверов, ключевых слов и размера содержимого.

Список разрешенных и заблокированных веб-сайтов позволяет блокировать веб-сайты на основе ключевых слов или разрешить доступ к проверенным безопасным веб-сайтам.

Политики использования реализуют в рамках локальной сети организации гибкие ограничения на основе диапазонов IP-адресов, типов содержимого или протоколов.

АЩИТА ОТ ВХОДЯЩИХ И ИСХОДЯЩИХ УГРОЗ

- Знаменитая система распознавания, очистки и карантина вирусов
- Интеграция с правилами брандмауэра Microsoft и веб-кэширование посредством антивирусного интерфейса Microsoft (ISAPI) в целях оптимизации и повышения скорости сканирования
- Сканирование файлов и веб-содержимого для обеспечения защиты в режиме реального времени и минимизации риска распространения вирусов в корпоративной сети
- Простые в управлении списки блокируемых веб-сайтов и FTP-серверов с синтаксисом на основе ключевых слов, а также списки разрешенных веб-сайтов

ПТИМИЗАЦИЯ, УПРАВЛЕНИЕ И ОТЧЕТНОСТЬ

- Загрузка системы при администрировании снижается благодаря централизованному управлению оповещениями за счет интеграции оповещений BitDefender в модуль оповещений ISA-сервера
- Поддержка среды ISA-серверов, настроенных как массив в контексте работы с большими объемами трафика при использовании в целях распределения нагрузки
- Технология оптимизации работы браузера посредством сканирования и разбивки крупных файлов на блоки небольшого размера
- Отчеты об активности вирусов, статистика сканирования и учет интернет-трафика
- Настраиваемые действия для различных событий, вызывающих оповещение по электронной почте или выполнение других действий
- Обеспечивает удаленное управление и настройку посредством консоли централизованного управления

Bitdefender®