

Достаточно ли корпоративного файрвола для защиты моих внешних корпоративных коммуникаций от вирусов и угроз?

ISA (Internet Security and Acceleration) – это корпоративный файрвол и прокси-сервер, разработанный компанией Microsoft. В дополнение к администрированию Интернет-доступа сотрудников, ISA-сервер позволяет отключать протоколы и коммуникационные порты, которые не являются необходимыми, но при этом уязвимы для атак. Тем не менее, ISA-сервер нуждается в дополнительном компоненте, который анализирует проходящий через протоколы периметра сети трафик и фильтрует опасные элементы или непродуктивный контент (например, спам).

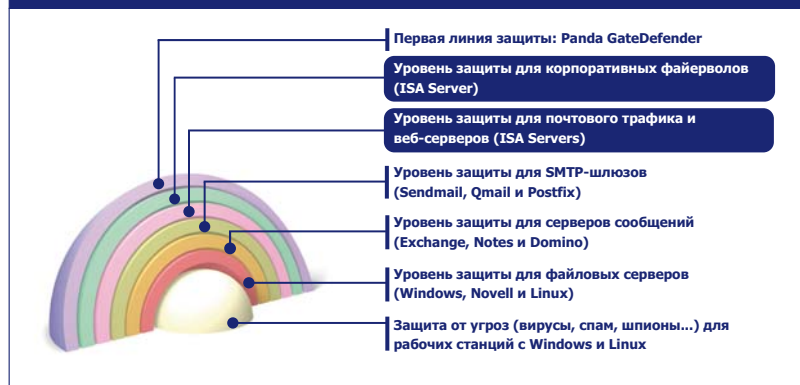
Вам необходимо интегрированное с ISA-Server решение, которое блокирует вредоносные программы

Panda Security for ISA Servers – это система защиты от вредоносных программ, которая благодаря использованию веб (ISAPI) и фильтра приложения сканирует и лечит все форматы проходящих через сервер Microsoft ISA файлов, отправленных и полученных через HTTP, SMTP и FTP (на HTTP).

Данное антивирусное решение защищает от вирусов, червей, троянцев, шпионского и рекламного ПО, хакерских утилит, фишинга, дозвончиков и рисков безопасности. Panda for ISA Servers является отличным дополнением к той защите, которая предоставляется модулем безопасности и прокси-кэшем в серверах MS ISA. В дополнение к этому продукт содержит инновационный модуль фильтрации контента.

Стратегия многоуровневой защиты

Panda Security for ISA Servers защищает периметральные слои веб-браузинга и корпоративный файрвол.



Основные выгоды

- Предоставляет **простое и централизованное управление**, внедрение, мониторинг и определение политик безопасности.
- Позволяет **принимать решение в режиме реального времени**.
- **Защищает** Ваши ISA-сервера **на всех уровнях**.
- **Повышает производительность** администратора и конечного пользователя.

Ключевые характеристики

- **Надежная защита электронной почты SMTP** от спама и фишинговых атак. Решение способно дезинфицировать вирусы во вложенных сообщениях и сжатых файлах на всех уровнях.
- **Гибкая фильтрация контента** с настройкой VIP-пользователей для использования Интернета и электронной почты SMTP.
- **Оптимизированная производительность** благодаря комбинированному использованию технологий PartFile и VirtualFile, и поддержкой 64-битных процессоров.
- **Мощный эвристический движок для веб-страниц**, позволяющий обнаруживать вирусный код не только в HTML-коде, но также и в файлах, загруженных на веб-странице.
- **Удаленное централизованное администрирование** сети с различными сканированиями сервера, графическими отчетами и централизованным карантинном для управления подозрительными объектами.
- **Полностью автоматические ежедневные обновления** сигнатурного файла.
- **Гибкие настройки** для индивидуализации предупредительных сообщений.



Надежная защита почты от атак

Panda for ISA предотвращает распространение инфекций через электронную почту. Обнаруживает фишинг и вложенные ложные сообщения на различных уровнях вложения, сжатые форматы ZIP, ARJ и др. Продукт **обнаруживает сетевые вирусы в пакетах** и другие вирусы в OLE-объектах, вставленных в тело сообщения.

В дополнение к этому, продукт полностью **удаляет инфицированное сообщение**, если оно автоматически генерируется червем, т.к. никакое подобное вложение или сообщение не несет ценности для получателя.

Контент-фильтр SMTP-почты и HTTP-трафика

С контент-фильтром для SMTP почты Вы можете фильтровать **зашифрованные сообщения**, создавать правила фильтрации с комбинацией нескольких критериев (тема и тело сообщения, имя, расширение и содержание вложения) с целью уничтожения внешних обращений, подозрительных сжатых файлов или нежелательных отправителей.

HTTP-фильтр **Panda for ISA** позволяет определенным IP-адресам и VIP-пользователям при использовании Интернета скачивать файлы без каких-либо ограничений, также как и осуществлять импорт черных списков компьютеров, которые не должны получить доступ к веб-страницам.

Продукт включает систему фильтрации по используемым паролям или макросам, размеру, расширению, имени или MIME-типе скаченных файлов. Модуль также гарантирует, что Java-апплеты, ActiveX-компоненты и скрипты будут заблокированы до их попадания к пользователям.

Оптимальная производительность

Технология Panda *VirtualFile* **сканирует в памяти все файлы**, в т.ч. и сжатые, намного быстрее, чем если бы сканирования осуществлялось с жесткого диска.

Продукт содержит технологию *PartFile*, которая позволяет сетевому администратору контролировать баланс производительности/безопасности на ISA-сервере, осуществляя сканирование и лечение только подозрительных файлов.

Мощный эвристический движок

Мощный и усовершенствованный движок HTML-сканирования способен определять и обезвреживать вирусы и вредоносные объекты, скрытые на веб-страницах, до того как они попадут к пользователям внутренней сети.

Panda for ISA содержит движок *Genetic Heuristic Engine (GHE)*, мощные возможности которого высокоэффективны в обнаружении неизвестных угроз. Продукт позволяет помещать подозрительные объекты на карантин на период, пока Panda не сможет их вылечить автоматически.

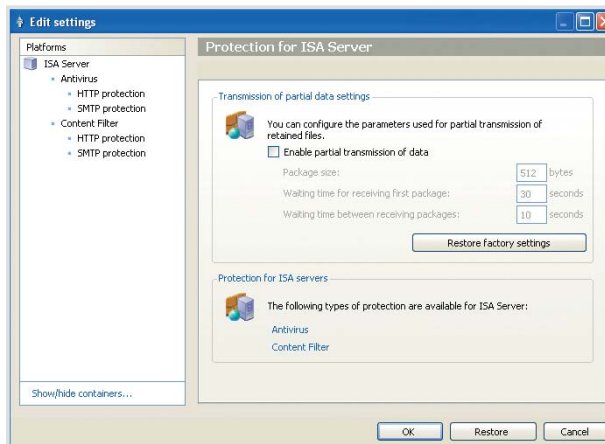
Удаленное централизованное управление

Panda for ISA управляется удаленно и централизованно через единую консоль **Panda AdminSecure**, благодаря которой все решения Panda могут устанавливаться, настраиваться и контролироваться с помощью отчетов, предупреждений и обзоров в режиме реального времени.

Так, вместо индивидуального управления каждого сервиса или защиты (антивирус, антиспам, антишпион), установленного на сервере, только единая консоль **Panda AdminSecure** способна непрерывно администрировать все объекты защиты, даже когда развернуты гетерогенные платформы доступа.

Автоматические ежедневные обновления

Panda for ISA может быть настроен так, чтобы автоматически проверять обновления каждый час и обновляться без вмешательства со стороны пользователя. Инкрементные обновления способствуют снижению использования полосы пропускания и сглаживанию коммуникационных пиков.



Гибкая настройка

Администраторы получают предупреждения непосредственно через SMTP почту или внутри сети через сообщения, отображаемые на экране. Предупреждения могут быть настроены с требуемыми параметрами, которые позволят предотвратить перегрузку сети.

Технические требования

Консоль Panda AdminSecure

Pentium II 266 МГц и выше.

ОЗУ: 140 МБ.

Жесткий диск: 140 МБ.

Internet Explorer 5.5.

Windows Installer 2.0.

Операционные системы: Windows 2000 / XP / XP 64-bits, Windows NT4 SP6 и Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bits, Windows Vista 32-bits / 64-bits, Windows Server 2008 (32 и 64 bits).

Panda Security for ISA Servers:

ISA Server 2004 Standart или Enterprise.

Pentium III 500 МГц или выше.

Минимум 1 Гб ОЗУ.

Локальная NTFS с минимум 180 Мб жесткого диска плюс 60 Мб для cache web content.

ISA Server 2006 Standart или Enterprise

Pentium III 733 МГц.

Минимум ОЗУ: 1 Гб.

Локальная NTFS с минимум 180 Мб жесткого диска плюс 60 Мб для cache web content.

Операционные системы: Windows 2000 Server, Advanced Server SP4 (или выше) или Windows Server 2003/R2.

"Для всех нас, кто получает много почты, наличие установленного Panda Antivirus дает гарантию того, что вирусы не будут распространяться по нашей сети!"

Иниго Ариас. Директор по маркетингу сети гипермаркетов. Eroski Group, Испания.



Помните, что **Panda Security for ISA Servers** может быть приобретен отдельно или в составе **Panda Security for Enterprise**.

Посетите www.pandasecurity.com

Получите Вашу демо-версию Panda Security for ISA Servers.

PANDA
SECURITY

20th Anniversary
1990-2010