

Panda GateDefenderIntegra

Объединенная защита бизнеса



Интернет-угрозы, которые становятся все более многообразными и сложными, следует блокировать до их проникновения в сеть во избежание вреда для Вашей организации.

Примерно 99% угроз, поражающих корпоративные сети, попадают из Интернета, что делает интернет-шлюз самой уязвимой точкой сетевой безопасности. Защита шлюза значительно уменьшит возможные проблемы до их проникновения во внутреннюю сеть.

Интернет-угрозы можно разделить на две группы:

- Угрозы сетевого уровня (несанкционированные соединения, вторжения, кража данных и т.д.)
- Контентные угрозы (вирусы, черви, шпионы, спам и т.д.).

"Вопросом выживания для разработчиков AV-решений является постоянный поиск новых путей усовершенствования их продуктов для более эффективной борьбы против новых угроз. Принцип Коллективного разума, основанный на "облачных" технологиях, - это следующий большой шаг в данном направлении. Я полагаю, что каждый AV-вендор будет обязан реализовать подобный подход в своих продуктах, чтобы выжить на антивирусном рынке".
Эндрю Джеки, аналитик Yankee Group



Решение: Panda GateDefender Integra

Panda GateDefender Integra - это устройство безопасности, объединяющее при помощи единого простого интерфейса несколько видов защиты периметра сети от всех типов Интернет-угроз как сетевого уровня, так и контентного. Устройство предлагает следующие типы защиты:

- **Файервол:** Помогает внутренним и внешним коммуникациям соответствовать политике безопасности.
- **Система предотвращения вторжений (IPS):** Защищает сеть от вторжений.
- **VPN:** Защищает важную информацию, передаваемую через Интернет.
- **Антивирус:** Защищает от всех типов вредоносного ПО.
- **Контент-фильтр:** Позволяет компаниям определять критерии, основанные на определении политик безопасности.
- **Антиспам:** Защищает от спама и нежелательной почты.
- **Веб-фильтр:** Ограничивает доступ к веб-контенту, не связанному с работой.



Две различные модели устройства отвечают потребностям малого бизнеса:

Модель устройства	Кол-во пользователей	Пропускная способность файервола	Параллельные сессии	10/100/1000 порты Ethernet
 100	До 100	330 Мбит/сек	350	4
 300	До 250	850 Мбит/сек	550	8

Основные преимущества

- **Включи и забудь.** Решение не требует настройки. С первой минуты после подключения Вы находитесь под его защитой.
- **Упрощает процесс управления безопасностью,** объединяя ВСЕ необходимые функции при помощи дружелюбного интерфейса.
- **Минимизирует операционные расходы,** предлагая практически самостоятельную защиту благодаря автоматическим обновлениям и графическим отчетам активности в режиме реального времени.
- **Помогает соответствовать корпоративным стандартам безопасности,** предотвращая потерю важной информации с помощью контент-фильтра и управления профилями безопасности пользователей.
- **Увеличивает продуктивность сотрудников** благодаря удалению спама и ограничению доступа к неотносящемуся к работе веб-контенту.
- **Предотвращает потерю важной информации** благодаря контролю входящего и исходящего трафиков и даже шифрованию передаваемой через Интернет информации.

Ключевые характеристики

- **Единственное устройство, работающее по принципу «Включи и забудь».** Оно по умолчанию включает антивирусную защиту, антиспам и модуль веб-фильтрации, защищая Ваш ПК с первой минуты работы и не требует конфигурирования.
- **Полная защита** от всех угроз. Содержит лучшую, разработанную зарекомендовавшими себя разработчиками защиту от вредоносных программ и потенциальных рисков (Panda), спама (Cloudmark) и нежелательного веб-контента (Cobion) наряду с защитой сетевого уровня, такой как Файервол с глубокой проверкой пакетов, IPS с широкими возможностями и VPN-сервер. Это позволяет объединить всю безопасность сети в единой точке.
- **Непрерывные автоматические обновления.** Правила и сигнатуры обновляются каждые 90 минут для антивируса, ISP или Веб-фильтра и каждую минуту для антиспама, снижая риски безопасности.
- **Оптимизация использования сетевых ресурсов.** Ограниченный доступ к непродуктивным веб-страницам оптимизирует использование полосы пропускания, а 98%-ая эффективность при обнаружении спама снимает значительную нагрузку с почтовых серверов и внутренней сети.
- **Проактивная защита контента.** Устройство в соответствии с определенной политикой безопасности проверяет входящий и исходящий трафики на предмет наличия потенциально опасного контента. Все коммуникации могут быть зашифрованы с помощью VPN.

Защита на уровне шлюза

Программно-аппаратное устройство Panda GateDefender Integra разработано для предоставления максимальной защиты и производительности на уровне шлюза. Сканирует самые широко используемые протоколы в реальном времени:

- HTTP, FTP, SMTP, IMAP4, POP3 и NNTP для защиты контента
- IP, TCP, UDP и ICMP для защиты от сетевых вторжений
- IPSec, SSL, L2TP и PPTP для VPN.

Максимальный контроль



Файрвол контролирует все коммуникации между сетью и Интернетом или между всеми подсетями, пользователями, группами и т.д.

Существует два типа фильтрации:

1. **Статический на уровне сети**, основанный на правилах, определенных администратором для входящего и исходящего трафика.
2. **Динамический на уровне приложений**, включая:
 - a. **“Проверка состояния”**: отслеживает статус и содержание основных коммуникаций во всех протоколах, а также статус, простои, установленные соединения и пр. в коммуникациях, осуществляемых с помощью FTP, PPTP, L2TP, IPSEC.
 - b. **“Глубокое инспектирование пакетов”**: сканирует содержание пакетов для проверки сообщений в HTTP, FTP, SMTP, IMAP, POP3 и т.д., когда другие модули доступны.

Безопасные коммуникации



VPN предоставляет безопасные коммуникационные туннели с удаленными пользователями или офисами через Интернет с помощью передачи зашифрованной отправителем информации и ее последующей дешифрацией получателем.

Работает в различных конфигурациях (хост-хост, хост-сеть, сеть-сеть) и поддерживает протоколы IPSec, SSL, L2TP и PPTP в серверном и клиентском режиме.

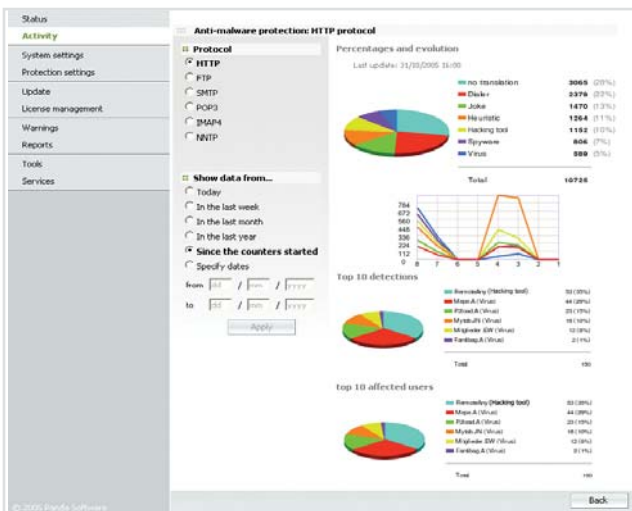
Усиленная безопасность



IPS предотвращает мгновенное распространение внешних атак, сканируя протоколы IP, ICMP, TCP и UDP с применением специальных правил.

Администраторы могут устанавливать пороговое значение каждого правила для снижения уровня ложных срабатываний, а также настраивать их для автоматической блокировки обнаруженных вторжений.

производительность пользователей, предотвращая доступ к нежелательным и не относящимся к работе веб-страницам.



Revision 1.06 2009

Система мониторинга в реальном времени

Консоль предоставляет в реальном времени графические отчеты об активности каждого вида защиты. Также можно настроить суммарные периодические отчеты и специализированные отчеты для каждого вида защиты.



Полная превентивная защита

Panda GateDefender Integra обнаруживает и блокирует все типы Интернет-угроз до их проникновения в сеть. Устройство защищает от

вирусов	червей	шпионов
фишинга	дозвончиков	хакерских утилит
троянов	шуточного ПО	рисков безопасности

Устройство также способно обнаруживать неизвестные угрозы благодаря своему генетическому эвристическому движку и принципу Коллективного разума.

Соответствие безопасности



Защита в виде контент-фильтра позволяет администраторам определить корпоративные политики безопасности. Можно установить, какие типы файлов и/или электронных писем могут быть получены или отправлены из сети. Это позволяет предотвратить утечку важной информации и другие потенциальные риски.

Блокировка спама



Модуль антиспама в Panda GateDefender Integra предотвращает перегрузку сети, блокируя спам на входе в сеть. Система также классифицирует сообщения как “Спам” или “Возможно спам”, позволяя применять к ним различные соответствующие действия.

Оптимизированное использование веб-ресурсов



Благодаря веб-фильтрации, устройство повышает производительность пользователей, предотвращая доступ к нежелательным и не относящимся к работе веб-страницам.

Администратор может выбрать любые из 60 категорий сайтов, которые могут быть доступны для пользователей сети, либо недоступны им, либо доступны только VIP-пользователям.

Централизованный мониторинг

Система отправляет настраиваемые предупреждения о событиях через SMTP, SNMP и/или Syslog. Администратор может выбрать, какие из событий могут быть отправлены при помощи каждого способа.

Автоматические обновления

Сигнатурный файл для антивируса и контент-фильтра, база данных для веб-фильтра и файл правил для IPS обновляются автоматически каждые 90 минут. Шаблоны для антиспама обновляются каждую минуту для того, чтобы гарантировать самую высокую степень обнаружения.

