Обзор устройств безопасности электронной почты IronPort

WHITE PAPER

СОДЕРЖАНИЕ

Вступление

Устройство IronPort типа «все в одном» сочетает в себе специализированный MTA, превентивную и реактивную защиту, контроль почтовой системы.

Электронная почта стала доминирующей формой делового общения – соперничая с (если не превосходя по важности) голосовой связью. В самом деле, электронная почта приобрела такое огромное влияние, что, как и в случае с факсом и банкоматом, стало сложно представить себе жизнь до ее широкого применения в течение последнего десятилетия. Распространенность этого средства передачи информации также привлекла большое и постоянно растущее количество угроз безопасности – спам, подделка писем, вирусы, регулятивные нарушения и кража интеллектуальной собственности.

Объемы и изощренность угроз безопасности электронной почты продолжают расти с неудержимой скоростью. Большинство клиентов констатируют, что около 90 процентов их входящей почты — плохие письма (спам, вирусы, и т.д.) и общее количество входящих писем удваивается с каждым годом, даже если число сотрудников остается постоянным. Эти угрозы безопасности электронной почты подпитываются мотивацией получения огромной прибыли, связанной со спамом, подделкой писем и кражей информации. Это создает ресурсы, которые привлекают профессиональных инженеров в бизнес разработки новых угроз, еще более обостряя ситуацию. Похоже, что эти процессы не имеют естественного равновесия, поэтому ожидается, что в обозримом будущем угрозы будут продолжать расти в объемах и изощренности.

Устройства безопасности электронной почты IronPort созданы для защиты сетей от сегодняшних и завтрашних почтовых угроз. Эти устройства построены на собственной операционной системе IronPort–AsyncOS™. Оптимизированная для передачи сообщений AsyncOS является фундаментом, который позволяет одному устройству IronPort обрабатывать почту более чем в десять раз эффективнее, чем традиционные системы, основанные на Unix. На вершине этой отлично масштабируемой платформы IronPort предлагает множество приложений безопасности для фильтрации спама и вирусов, сканирования контента и введения политик. В данном решении присутствуют как уникальные технологии, разработанные компанией IronPort, так и тесно интегрированная технология фильтрации от партнеров, являющихся лучшими в своем деле. Модульная архитектура системы позволяет включать и выключать эти приложения в соответствии с потребностями каждого клиента.

Ниже приведен технический обзор основных компонентов устройства безопасности электронной почты IronPort по разделам.

- Фундамент – AsyncOS
- Улучшенная структура очереди и управление подключениями
- Аутентификация почты
- SenderBase®
- Репутационная фильтрация (Reputation Filtering™) и контроль потока
- Virus Outbreak Filters™
- Сканирование контента и введение политик
- Анти-спам, основанный на содержании
- Анти-вирус, основанный на сигнатурах
- Управление, мониторинг и отчетность
- Централизованное управление

ФУНДАМЕНТ – ASYNCOS

Многие из ограничений традиционных программных шлюзов, основанных на Unix, заключаются не в самих приложениях, а в том, как приложение взаимодействует с операционной системой. Для борьбы с этими ограничениями IronPort разработали уникальную операционную систему AsyncOS, специализированную под асинхронную задачу передачи электронных сообщений.

Электронная почта – это средство передачи информации с высокой интенсивностью подключений. Любая сеть умеренных размеров может запросто иметь тысячи параллельных входящих и исходящих почтовых подключений. Эти подключения зачастую относительно медленны, так как могут иметь на другом конце Интернета занятый сервер. Традиционный MTA имеет проблемы с высоким числом параллельных подключений. Большинство традиционных MTA, работающих на операционных системах общего назначения, таких как Unix или Windows, ограничены одной или двумя сотнями параллельных подключений, потому что операционная

система ограничивает число потоков, которые могут быть открыты одновременно. Традиционная модель поточности требует наличия выделенного стека памяти для каждого потока, и система не может предоставить больше памяти для открытия новых потоков. AsyncOS от IronPort предоставляет безстековую модель поточности, которая не нуждается в большом стеке памяти для каждого потока, позволяя MTA IronPort поддерживать массивный параллелизм – 10 000 одновременных подключений – в 100 раз больше, чем традиционные MTA.

Такой массивный параллелизм гарантирует, что при использовании в любых практических целях IronPort никогда не достигнет предела подключений. Решение проблемы параллелизма означает, что узким местом становится ввод/вывод данных. Так как все сообщения в MTA должны сохраняться на диске, MTA – система с интенсивным вводом/выводом.

Проблема ввода/вывода решается в AsyncOS двумя способами. Первый – с помощью планировщика ввода/вывода. AsyncOS использует асинхронную природу сообщений для их обработки в оптимальном порядке. Если поток активно использует ввод/вывод, система позволит ему завершить это действие, и не будет вмешиваться, используя планировщик. Это значительно увеличивает эффективность системы ввода/вывода.

Вторая оптимизация ввода/вывода заключается в файловой системе AsyncOS. Традиционные MTA используют файловую систему для сохранения состояния приложения. Если домен–получатель становится недоступным, то очередь адресованных ему сообщений начинает расти, и задержки из-за традиционной файловой системы замедляют работу всей системы. А когда домен-получатель вновь становится доступным, MTA должен возобновить доставку сообщений и очистить очередь. В этот момент система требует максимальной пропускной способности для очистки очереди, а задержки из-за файловой системы делают эту пропускную способность минимальной. Так что очередь растет, приводя к все большим задержкам. Все это в конце концов приводит к тому, что система сбоит и требует вмешательства администратора.

УЛУЧШЕННАЯ СТРУКТУРА ОЧЕРЕДИ И УПРАВЛЕНИЕ ПОДКЛЮЧЕНИЯМИ

На базе оптимизированной операционной системы IronPort разработал полностью новую архитектуру MTA. Устройство IronPort содержит уникальную структуру независимых очередей. Система поддерживает отдельную очередь для каждого из доменов. Она также поддерживает осведомленность о состоянии всех доменов-получателей. Если большой домен (например, Hotmail) становится недоступным, система его помечает соответствующим образом, и все новые сообщения от серверов groupware помещаются в очередь для этого домена. Но помещение в отдельную очередь сообщений для недоступного домена не инициирует цикл повтора доставки для каждого нового сообщения. Вместо этого устройство безопасности электронной почты IronPort хранит все сообщения для недоступного домена и выполняет один глобальный повтор доставки для этого домена. Когда домен-получатель становится доступным, все сообщения доставляются. Это решает общую проблему всех традиционных

MTA. Их часто парализует большое число повторов доставки для популярного узла, который недоступен.

Таким же образом MTA IronPort способен планировать повтор доставки на основе домена. Это решает другую распространенную проблему MTA: большое число возвратов сообщений (bounces), которые замедляют очередь. Обычно атаки спамеров включают большое количество несуществующих почтовых адресатов. Эти возвраты сообщений часто отправляются на домен, который эти сообщения на самом деле не отправлял, приводя к замедлению работы традиционных MTA почтой, которая изначально была мусором. Это зачастую требует вмешательства администратора, сортировки очереди, уничтожения всех сообщений, предназначенных для этого домена. Настраивая повторную отправку для каждого из доменов, администраторы могут установить количество таких повторов равным нулю для подозрительных доменов и позволить устройству автоматически очищать такие сообщения. Эти возможности позволяют устройству IronPort действовать в качестве “амортизатора” для серверов groupware, управляя очередью сообщений без вмешательства.

Устройства IronPort также обладают уникальной технологией, называемой Virtual Gateway™. Эта технология позволяет определять и классифицировать различные IP-адреса для исходящей почты. Она может использоваться для разделения исходящей почты, адресованной различным организациям, по разным исходящим IP-адресам. Технология Virtual Gateway™ – это мощное средство для решения проблем доставки. Если один из исходящих почтовых потоков не понравился провайдеру и блокируется, то блокировка будет распространяться только на этот IP-адрес, который стал причиной блокировки, позволяя почте беспрепятственно идти по другим потокам. Эта возможность пригодится провайдерам – каждому из клиентов можно предоставить свой уникальный IP-адрес, гарантируя, что ни один из клиентов не повлияет на работу почты другого. Также эта технология может использоваться для разделения коммерческой почты и личной почты сотрудников. Этот подход локализует проблемы с одним из потоков.

Система очередей IronPort создает отдельные очереди для каждого домена-получателя, для каждого виртуального шлюза. Таким образом, популярный домен-получатель (как Hotmail) может иметь отдельную очередь для каждого из виртуальных шлюзов, гарантируя, что если один из шлюзов заблокирован, второй продолжит доставку почты. Виртуальные шлюзы также могут использоваться для приоритезации срочной почты. Отправляя эти сообщения через отдельный шлюз, Вы поставите их в свою отдельную очередь, в которой они не будут замедляться письмами с низким приоритетом.

Вдобавок к улучшенной организации очередей и управлению возвратом сообщений MTA IronPort обладает превосходным управлением подключениями. Система группирует все сообщения, направленные на общий домен. Она отправляет несколько сообщений на одно подключение, и открывает множество подключений к одному узлу. Традиционные MTA будут открывать новое подключение для каждого сообщения, повышая издержки получающего и передающего MTA.

Алгоритм IronPort “Good Neighbor” вычисляет общую скорость передачи

данных для всех подключений к данному домену. Когда скорость передачи данных начинает стабилизироваться, IronPort обрывает самое новое подключение, чтобы не перегружать удаленный сервер. Устройство IronPort обладает своим DNS-кэшем, что значительно повышает производительность. Этот кэш будет хранить все IP-адреса всех MX для домена-получателя и распределять подключения по разным MX – в соответствии с их приоритетами.

АУТЕНТИФИКАЦИЯ ПОЧТЫ

Несмотря на то, что отсутствие аутентификации почты не использовалось в течение двадцати лет, злоупотребление этим недостатком за последние несколько лет значительно возросло. Сегодня около восьмидесяти процентов всей почты – это спам, причем в большинстве случаев с поддельной информацией об отправителе. Подделка домена отправителя позволяет красть интеллектуальную собственность и создавать распределенные DoS-атаки на основе возвратов сообщений. Возвраты сообщений становятся растущей проблемой для администраторов почты. Спамеры часто отправляют сообщения с поддельным обратным адресом, которые содержат спам или вирус. И ответ о невозможности доставки придет именно на этот поддельный адрес (им может быть и ваш адрес) с вложенным спамом или вирусом. IronPort Bounce Verification™ предоставляет администраторам средства для защиты от атак возвратами сообщений (bounce attacks) с минимальными потерями. Bounce Verification вставляет цифровую подпись в адрес отправителя каждого исходящего письма (SMTP Mail From:).

Обычно адрес отправителя выглядит так:

MAIL FROM: support@bigbank.com

Bounce Verification изменяет его на:

MAIL FROM: pvrs=support=3201EA1CF@bigbank.com

Когда устройство получает возвраты сообщений, наличие правильной подписи поможет отличить настоящие возвраты от поддельных.

Решение IronPort предоставляет дополнительные функции для поддержки удаления, пометки или помещения в карантин поддельных возвратов сообщений.

Уникальность технологии Bounce Verification в том, что, в отличие от других технологий аутентификации почты, для эффективной работы она не требует глобального внедрения. Однонаправленность технологии IronPort Bounce Verification приносит немедленную пользу тому, кто ее использует.

Устройства безопасности электронной почты IronPort поддерживают технологию DomainKeys. В схеме DomainKeys отправитель создает хэш для каждого из исходящих сообщений и шифрует его, используя секретный ключ из пары PKI. Общий ключ из этой пары публикуется в виде текстовой записи DNS для домена этого отправителя. Сервер-получатель аутентифицирует это сообщение, получая домен отправителя из сообщения, общий ключ из DNS-записи отправителя, и сравнивая

подпись с содержимым сообщения. Письмо с правильной подписью аутентифицируется, а с неправильной – нет. Хотя этот протокол гибок, DKIM почти всегда проверяет домен в заголовке "From:". Так как этот заголовок в почтовых клиентах всегда виден конечным пользователям, эта технология является прекрасным решением проблемы фишинга.

Устройство IronPort включает высокопроизводительный клиент LDAP. Адреса входящих сообщений могут проверяться в любой директории LDAP, такой как Microsoft Active Directory. Адреса могут проверяться как в ходе SMTP-общения (с отправкой возврата сообщения еще до принятия самого сообщения), так и после принятия сообщения с отправкой NDR (non-delivery report) отправителю. Однако такой сценарий имеет недостаток – он помогает спамерам определить существование реального почтового адреса. Это стало причиной того, что многие корпорации приняли политику задержки возврата сообщений (в течении SMTP-сессии принимаются все сообщения).

Для решения этих проблем IronPort использует технологию Directory Harvest Attack Prevention (DHAP). Технология DHAP следит за числом неправильных адресатов от данного отправителя. Как только этот отправитель превышает определенный администратором уровень неправильных адресатов (допустим, десять неверных адресов в час), отправитель считается злоумышленником, и почта от него блокируется без генерации NDR и кода ошибки. Этот уровень может быть настроен по-разному в зависимости от репутации отправителя (более детальное описание системы репутационной фильтрации IronPort следует дальше). Плохие или подозрительные отправители могут иметь низкий уровень DHAP, проверенные – высокий.

Система DHAP от IronPort позволяет администраторам безбоязненно использовать возврат писем. Если администратор предпочитает использовать задержку отправки возврата писем, система DHAP значительно уменьшит количество ложных возвратов писем, сгенерированных спамерами.

SENDERBASE – ПЕРВАЯ, САМАЯ БОЛЬШАЯ, ЛУЧШАЯ БАЗА РЕПУТАЦИЙ

SenderBase – это первая и самая большая в индустрии сеть мониторинга почтового и Web-трафика. SenderBase отслеживает множество сетевых параметров каждого из IP-адресов, отсылающих почту в Интернет. Эти параметры включают общие объемы почты, отосланной этим IP-адресом, как давно он отсылает почту, его местоположение, присутствие в черных или белых списках, правильность настройки DNS, способность отправителя принимать почту, и так далее.

SenderBase собирает данные приблизительно из 100 000 различных сетей по всему миру. Эти сети представляют более 25 процентов мирового почтового и Web-трафика. SenderBase – это единственная служба мониторинга трафика, которая собирает данные из разных источников, как из базы клиентов IronPort, так и вне ее. SenderBase отслеживает более 120-ти различных параметров о каждом данном отправителе.

SenderBase использует алгоритм, который анализирует эти объективные параметры сетевого уровня и формирует “reputation score” (рейтинг отправителя) от -10 до +10. Этот рейтинг затем становится доступным для устройства в режиме реального времени во время получения сообщения от любого отправителя. Множество политик могут быть привязаны к рейтингу отправителя, начиная с уровня DHAP до параметров контроля потока, размеров вложения и типов файлов.

Много технических специалистов и статистиков, говорящих на многих языках, работают в 24x7 IronPort Threat Operations Center (TOC), они анализируют данные в SenderBase и управляют ими. Команда TOC разработала процессор качества данных, который обрабатывает и взвешивает данные из различных источников для точной и аккуратной интерпретации. Эта команда следит за тем, чтобы данные в SenderBase были свежими и точными, и администраторы могли опираться на данные из SenderBase для автоматической классификации почты, избегая затрат времени и ресурсов на составление черных и белых списков.

РЕПУТАЦИОННАЯ ФИЛЬТРАЦИЯ И КОНТРОЛЬ ПОТОКА

Устройство IronPort производит проверку репутации каждого входящего сообщения, используя текстовую запись DNS (похоже на механизм RBL). Затем IronPort может применить уникальную политику безопасности почты к этому отправителю, основываясь на его рейтинге (это и есть репутационная фильтрация). Размер вложения, ограничения на тип и имя файла, схемы фильтрации спама, вирусов и контента, параметры контроля потока – все это применяется к отправителям на основе их рейтинга. Таким образом, подозрительный отправитель может получить очень ограниченные возможности. Например, подозрительному отправителю может быть разрешено присылать письма не более чем на десять адресов в час, с исполняемыми файлы во вложении, делать полную проверку его писем на спам, вирусы и ключевые слова. Напротив, проверенный отправитель получит щедрые привилегии – 1000 адресатов в час, вложения больших размеров и любых типов, шифрование TLS. Администраторы настраивают эти различные политики только раз (используя Web-интерфейс), потом просто наблюдая за тем, как система автоматически классифицирует отправителей. Многие администраторы будут производить ежемесячный обзор политик и потока почты, не заходя дальше этого.

Возможности контроля потока у IronPort уникальны. Большинство коммерческих систем, доступных сегодня, предлагают что-то вроде «замедления», ограничивая число подключений от одного узла. Спамеры легко обходят этот подход, отправляя множество сообщений за подключение или одно письмо множеству получателей. Система IronPort может ограничивать количество адресатов в час. Это очень эффективное решение, если оно связано с репутацией. Короче говоря, чем больше отправитель похож на спамера, тем медленнее он с нами работает. Возможность ограничения отправителей позволяет устройству справляться с «серыми» отправителями. Очевидные спамеры могут быть быстро

идентифицированы и блокированы. А письма проверенных отправителей могут доставляться без проверки на спам и вирусы. Эти два класса отправителей обычно составляют 80 процентов потока входящей почты. Остальные 20 ограничиваются в скорости и проверяются на спам и вирусы.

Система репутационных фильтров IronPort была первой и остается самой изощренной. При настройке по умолчанию она будет блокировать около 80-ти процентов входящей почты на этапе подключения, тем самым уменьшая трафик (сообщения с низким рейтингом не принимаются) и не загружая системные ресурсы. Требующие много процессорного времени фильтры спама и вирусов используются только при необходимости, а ограничение потока почты – очень эффективная защита от атак спамеров типа "hit and run" и DoS.

Контроль потока почты IronPort также очень полезен при управлении доставкой исходящей почты. Устройство IronPort – это высокопроизводительное устройство, но было создано в расчете на то, чтобы получающий домен не будет перегружен, что могло бы привести к внесению нас в черный список. Более того, ограничение скорости может использоваться и для внутренней маршрутизации почты. Почта, направленная на центральный сервер Microsoft Exchange или IBM Lotus Notes может доставляться с большой скоростью, а почта для удаленных офисов может замедляться для обеспечения общей стабильности системы.

IRONPORT VIRUS OUTBREAK FILTERS

Несмотря на то, что основанные на сигнатурах антивирусные системы устанавливаются уже давно, многие клиенты до сих пор имеют проблемы с вирусными атаками, которые распространяются до появления сигнатур. Причина этому – изначальная реактивность антивирусных сигнатур. Каким бы хорошим не был производитель антивирусных сигнатур, требуется определенное время для того, чтобы обнаружить, изолировать и охарактеризовать вирус. Далее требуется время на создание, тестирование и установку сигнатуры. Все эти задачи обычно требуют от 6 до 48 часов, в зависимости от атаки. В течение этого времени вирус будет активно распространяться по всему миру.

На сегодняшний день нет ни одной формы общения людей, при которой информация могла распространяться так быстро, как в случае с современным почтовым вирусом. IronPort Threat Operations Center (TOC) разработал алгоритмы, которые обнаруживают аномалии, такие как массовое появление новых отправляющих почту IP-адресов, которые до этого вообще не отправляли почту, и соответствующее увеличение объема сообщений с определенными размером, типом или именем вложения. Затем TOC автоматически генерирует оповещения и создает правило, утвержденное техническими специалистами TOC. Это правило затем автоматически отправляется на все устройства IronPort, и вся похожая на аномальную почта помещается в карантин. Системному администратору отправляется оповещение и информация об обновлениях состояния вирусной вспышки. Администраторы могут просматривать этот карантин и проверять на вирусы, удалять или отпускать сообщения. После обновления

сигнатур администраторы могут проверять сообщения снова, чтобы убедиться, что они безопасны, а затем отпускать сообщения в соответствии с настройками политики антивируса. Только система IronPort Outbreak Filters постоянно сканирует сообщения в карантине и оценивает их заново (на основании последних правил, идентифицирующих вирус), что приводит к минимальным шансам неправильной классификации. Затем динамический карантин IronPort автоматически отпускает сообщения, не соответствующие новым правилам. Динамический карантин обеспечивает незамедлительную защиту и высочайшую точность.

Технология IronPort Virus Outbreak Filters работает более полутора лет и уже достигла невероятных успехов, защищая в среднем за 16 часов до появления сигнатур, останавливая сотни миллионов зараженных сообщений, которые в противном случае дошли бы до рабочих станций. Время отклика на недавние атаки показано на Рисунке 1. Учитывая, что «Средние затраты на очистку от вируса в 2004-м году составили $130 000» (источник – ICSA Labs 10th Annual Virus Prevalence Survey), несложно оценить технологию Virus Outbreak Filters.

Рисунок 1. IronPort Outbreak Filters останавливает вирусы до появления сигнатур.

Вирус	Дата	Реакция VOF	Появление сигнатуры	Выигрыш Outbreak Filter
Zotob.C	16.08.2005	01:56	04:47	2 часа 51 минута
MyTob.G	16.08.2005	11:30	12:58 (следующего дня)	13 часов 28 минут
Sober.L	24.03.2005	16:10	18:23	2 часа 13 минут
Mydoom.BB	15.02.2005	18:08	22:54 (следующего дня)	28 часов 46 минут

СКАНИРОВАНИЕ КОНТЕНТА И СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Устройство IronPort обладает быстрой, гибкой и тонко настраиваемой системой фильтрации сообщений. Используя логику “if-then-else”, как в языке программирования C, можно создавать пользовательские фильтры, которые позволят администраторам реализовывать любые мыслимые требования. Параметры, которые могут быть использованы в поле “if”, включают IP-адрес отправителя и получателя, доменное имя или адрес, заголовки, репутацию отправителя или данные, доступные ему по LDAP. Допустимые действия включают в себя помещение в карантин, перенаправление, оповещение, тегирование, архивирование, возврат сообщения (bounce), и другие.

Примером такого фильтра может служить правило, которое гласит, что если сообщение отправлено определенному получателю (определяется адресом почты или запросом LDAP) или определенным отправителем, то ограничить размер вложения для него и сделать архивную копию. Эта способность очень важна, если имеешь дело с множеством различных требований больших компаний, и эти “специальные запросы” легко реализуются с помощью простых фильтров сообщений.

Самое распространенное применение фильтры сообщений нашли в

соответствии требованиям. IronPort создал готовые словари медицинских терминов для соответствия HIPAA. Также доступны словари для соответствия Sarbanes Oxley (SOX) и SEC. IronPort поддерживает шифрование TLS (Transport Layer Security), которое может выборочно применяться только к той почте, которая требует шифрования. Для более разносторонней фильтрации и шифрования IronPort поддерживает партнерские отношения с такими лидерами в этих областях, как PostX, PGP и Sigaba.

Фильтры могут создаваться как с помощью GUI (графический Web-интерфейс), так и с помощью командной строки, поддерживающей скрипты. После создания политик они управляются IronPort Email Security Manager™. Этот мощный Web-интерфейс предоставляет разносторонний взгляд на политики для всей почты, спама, вирусов, вложений и соответствия требованиям. Правила могут создаваться с четкой иерархией – правило по умолчанию и затем специфические правила в порядке выполнения. Для правильной обработки сообщений с несколькими получателями IronPort поддерживает разделение сообщений (message splitting) – получатели, соответствующие одному набору правил, группируются, получатели для других правил группируются и обрабатываются отдельно. Это очень важная функция в условиях управления политиками для больших компаний, где политики могут быть очень сложными. Email Security Manager делает такое управление простым.

ОСНОВАННЫЙ НА СОДЕРЖИМОМ АНТИСПАМ И АНТИВИРУС

IronPort обеспечивает разностороннюю защиту от спама, предоставляя две линии обороны: внешний превентивный слой (репутационные фильтры) и внутренние реактивные фильтры.

Система фильтров репутации IronPort – это первая линия обороны, которая блокирует до 80 процентов входящего спама на этапе соединения. IronPort Reputation Filters™ в режиме умолчания направляет почту от известных хороших отправителей прямо в почтовых ящик, избегая ненужных затрат ресурсов и риска ложного срабатывания антиспам-системы для заведомо хорошей почты. Но 20 процентов всей почты находится в “серой зоне”, и важно ограничивать в скорости эти письма и сканировать каждое из них. IronPort Anti-Spam™ призван справляться с этой “серой зоной”, используя самые продвинутые подходы обнаружения угроз в этой области. Вдобавок к анализу репутации отправителя, уникальная система IronPort Context Adaptive Scanning Engine™ (CASE) изучает весь контекст сообщения, включая:

- содержание,
- логическую структуру письма,
- репутацию ссылок в письме.

После комбинирования оценки CASE с репутацией отправителя конечный результат получается точнее, чем у традиционных технологий фильтрации спама. Технология IronPort Web Reputation™ изучает поведение и модель трафика web-сайта для определения его репутации. IronPort CASE получает репутацию любой ссылки внутри тела сообщения, так что

выполняется его более точный анализ. Все это позволяет системе IronPort Anti-Spam защитить пользователей от спама, фишинга и шпионского ПО, распространяющегося по почте.

Для организаций, которые предпочитают предоставлять управление спамом своим пользователям, устройства IronPort предлагают систему IronPort Spam Quarantine™. IronPort Spam Quarantine – это решение по самообслуживанию для конечных пользователей, с легким в использовании Web- или Email-интерфейсом. Эта технология предоставляет конечным пользователям свой контейнер для хранения сообщений, определенных как спам, и легко интегрируется с существующими почтовыми серверами и базами пользователей.

IronPort также обеспечен антивирусными сигнатурами от Sophos, которые полностью интегрированы в устройство IronPort и имеют возможности легкого управления и отчетности. Система Sophos anti-virus тесно связана с IronPort Virus Outbreak Filters, что делает возможным тестовое сканирование сообщений перед отпуском из карантина. IronPort и Sophos объединились с целью обнаружения и остановки вирусных атак с максимальной защитой для наших клиентов. Для максимальной производительности система Sophos использует сканирование сообщений в оперативной памяти. Сообщение сохраняется на диске, а затем неоднократно сканируется в оперативной памяти. Фильтры сообщений IronPort полностью интегрируются с базами пользователей, так что для одной группы LDAP (скажем, “engineering”) сообщения с вирусами удаляются, а для другой (скажем, “sales”) – помечаются и доставляются.

УПРАВЛЕНИЕ, МОНИТОРИНГ И ОТЧЕТНОСТЬ

IronPort предоставляет изощренные средства для управления, мониторинга и отчетности, разработанные для больших корпораций и провайдеров, которые составляют базу клиентов IronPort. Каждое устройство обладает уникальной системой отчетности реального времени Mail Flow Monitor™. Mail Flow Monitor предоставляет обзор всех входящих и исходящих подключений. Из Web-интерфейса IronPort Mail Flow Monitor системные администраторы могут легко просматривать активность в очередях сообщений. Здесь отображаются домены с максимальным числом сообщений в очереди с общей статистикой. На одной странице администраторы могут увидеть количество сообщений в очереди, число открытых подключений, успешных доставок, а также мягких и жестких возвратов писем (soft & hard bounces). По каждому из доменов можно посмотреть отдельную подробную статистику. Mail Flow Monitor покажет IP-адреса всех записей MX для домена, статус (up/down) этого домена, время последней попытки подключения, возраст самого старого сообщения в очереди для этого домена и подробности о возвратах сообщений или кодах ошибок, полученных от этого домена. Это многофункциональное средство позволяет администраторам быстро идентифицировать и исправлять ошибки. Для дополнительных проверок IronPort поддерживает “domain debug”, специальную функцию журналирования, которая позволяет сохранять каждую SMTP-сессию полностью только для определенного

домена. Это избавляет администраторов от необходимости обрабатывать огромные объемы логов для обнаружения ошибок. Более того, каждое из сообщений в очереди может быть направлено на любой удаленный узел или сервер, или просто удалено.

Для входящей почты Mail Flow Monitor показывает отправителей с наибольшими показателями количества писем, вердиктов по спаму и вирусам, репутации, указывает на аномалии в объемах почты. С его помощью администраторы могут проследить за любым подозрительным отправителем, посмотреть по нему более детальную статистику, включая его репутацию в IronPort SenderBase. Администраторы могут увидеть, вступило ли в действие ограничение скорости почты, и если да, то, как много сообщений было задержано. Эта возможность уникальна, так как большинство подходов к задержке писем просто замедляют подключение, так что нет возможности узнать, сколько сообщений было задержано. Если администратор хочет изменить политику, которая применяется к данному отправителю, он может сделать это просто из Mail Flow Monitor.

Вдобавок к мониторингу и отчетности в реальном времени, предоставленных Mail Flow Monitor, IronPort предлагает централизированную хронологическую систему обработки журналов Mail Flow Central™. Эта система получает данные журналов из множества устройств и загружает их в базу данных SQL. Mail Flow Central предоставляет мощные средства по обработке этих данных, генерации отчетов по ним, хронологическому анализу спама, вирусов и контентных фильтров. Также имеется мощное средство отслеживания сообщений, с помощью которого можно искать сообщения от определенного отправителя, с определенной темой, типом вложения, и т.д. Эта система облегчает работу системным администраторам, которым раньше приходилось выполнять поиск по файлам журналов на каждом из устройств в отдельности для нахождения определенного письма. Mail Flow Central – это программное обеспечение, которое может масштабироваться и устанавливаться по желанию клиента. Предлагается, чтобы Mail Flow Central был запущен на рабочей станции или сервере не в DMZ, чтобы не нагружать машину в DMZ журналами и поиском сообщений. IronPort также публикует схему Mail Flow Central для возможности создания пользовательских запросов.

Для важных системных функций IronPort предоставляет мониторинг как почты, так и SMTP-подключений. Состояние системы и события уровня безопасности приложений передаются через SMTP-ловушки и настраиваемые почтовые оповещения. Текущее состояние системы также доступно в виде XML. Команда инженеров IronPort Systems разработала множество скриптов, которые могут использоваться для выдачи выборочной системной информации в более крупные системы сетевого мониторинга.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Используя централизованное управление, в случае, если для одной из систем сделаны какие-то изменения, администратор может применить эти изменения и для другой системы, группы устройств или кластера. Эта

очень мощная и изощренная иерархическая система была разработана для мировых провайдеров и организаций с распределенной сетью. Она выполнена с использованием одноранговой смешанной сети, где конфигурация любой машины хранится на машинах того же ранга. Это дает гибкость, так как изменения могут быть сделаны для одной машины, а затем распространены по всему кластеру. Если любая из машин выходит из строя, новой машине присваивается ее IP-адрес, и эта новая машина автоматически свяжется с машинами из ее ранга и настроит себя сама. Вся информация о конфигурации системы доступна в виде файла XML для резервирования. Все действия администраторов заносятся в журнал, к которому есть три уровня доступа – только чтение, администратор и суперпользователь.

ЗАКЛЮЧЕНИЕ

Устройство безопасности электронной почты IronPort – это самая изощренная система в этой области из существующих сегодня. Система IronPort установлена у восьми из десяти крупнейших мировых провайдеров и у 20 процентов крупнейших мировых компаний, и продемонстрировала рекорды непревзойденной безопасности и надежности.

Та же функциональность, которая присутствует в самых мощных моделях IronPort, доступна и в облегченной серии IronPort C100™. Целью команды разработчиков IronPort является создание высокоинтеллектуальных и дееспособных систем, которые могут автоматически справляться со сложными ситуациями, такими как вспышки вирусов и сбой в работе основного почтового домена. Эти события обрабатываются автоматически, уменьшая затраты на администрирование более чем на 75 процентов. Многие администраторы сообщают, что им приходится прикасаться к устройствам IronPort лишь раз в месяц, “на всякий случай”. Причинами такой простоты управления являются продвинутые технологии, применяемые в устройствах IronPort, а также высочайший в мире уровень безопасности.

IronPort Systems – производитель ведущих продуктов в области безопасности электронной почты и Web, предназначенных как для малых организаций, так и для компаний из Global 2000. IronPort предоставляет высокопроизводительные, простые в использовании инновационные решения для тех, перед кем стоят задачи управления и защиты своих корпоративных сетей от Интернет-угроз.