Обзор технологии обеспечения безопасности web-трафика

Решение Cisco IronPort для обеспечения безопасности web-трафика данных и предотвращения потери данных

Безопасность данных и предотвращение потери данных (DLP) представляет серьезную проблему для компаний, поскольку число инцидентов, как и затраты на устранение их последствий, продолжает расти. Потеря данных может негативно сказаться на нематериальных активах компании и ее деловой репутации, снизить ее акционерную стоимость, повысить риск юридической ответственности и поставить частных лиц и организации перед опасностью кражи финансовых средств — независимо от того, является потеря данных результатом злонамеренного воздействия или случайной ошибки.

Будучи лидером в области обеспечения безопасности web-трафика, компания Cisco® осознает сложности создания решения, способного работать в условиях повсеместного доступа к Интернету, который является наиболее важным фактором риска потери данных. Наличие высокопроизводительного решения для обеспечения безопасности данных и предотвращения их потери, охватывающего все важнейшие сетевые протоколы, стало обязательным требованием для современных организаций. Лица, принимающие решения, вынуждены обращаться к таким поставщикам, как компания Cisco, которая обладает обширным опытом в области обеспечения безопасности и сканирования контента, и выбирать лучшее в своем классе решение, включающее технологии обеспечения безопасности данных и предотвращения их потери и поддерживающее интеграцию с внешними решениями DLP для реализации политик.

> «Расширенное использование технологий Web 2.0 (блоги, социальные сети и мгновенный обмен сообщениями потребительского уровня) повышает интенсивность выхода информации за пределы предприятия».

- *Эндрю Джекит (Andrew Jaquith), главный аналитик*
  Forrester Research

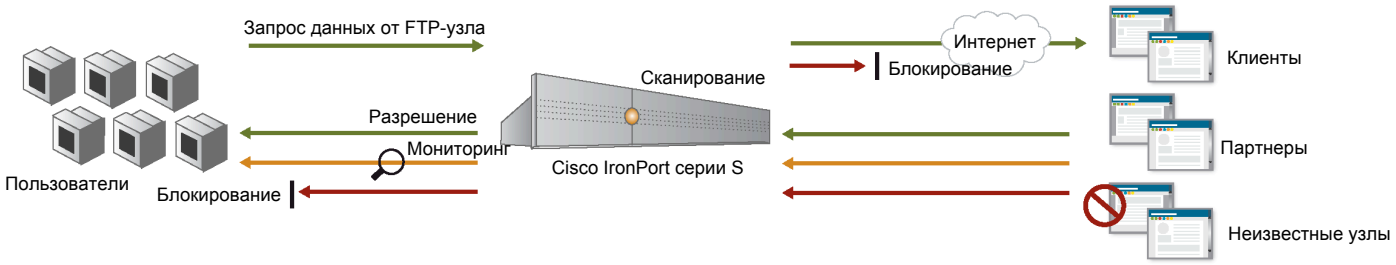
РЕШЕНИЕ CISCO IRONPORT ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ WEB-ТРАФИКА ДАННЫХ

Вредоносные программные средства, ориентированные на кражу данных, представляют реальную и неизбежную угрозу для современного бизнеса и обозначают начальную точку в любых обсуждениях безопасности данных в Интернете. Устройство обеспечения безопасности web-трафика Cisco IronPort обеспечивает наилучшую защиту от вредоносных программных средств для кражи данных, используя репутационные фильтры web-трафика Cisco IronPort Web Reputation Filters, механизм Cisco IronPort Dynamic Vectoring and Streaming (DVS) и монитор трафика 4-го уровня (L4TM). Эти технологии предотвращают проникновение троянских программ и других вредоносных приложений в сеть, одновременно блокируя вредоносный трафик существующих вредоносных программных средств (трафик «phone-home»).

Однако проблема потери данных выходит за рамки защиты от вредоносных программных средств. Сотрудники могут легко отправлять сообщения, содержащие закрытую информацию, по открытой электронной почте, публиковать конфиденциальные данные в социальных сетях и блогах, либо передавать финансовые документы на FTP-сервер, находящийся за пределами корпоративной сети. Предотвратить выход конфиденциальных данных за границу корпоративной сети, одновременно позволяя пользователям пользоваться всеми преимуществами работы в Интернете — это важная и сложная задача, требующая решения.

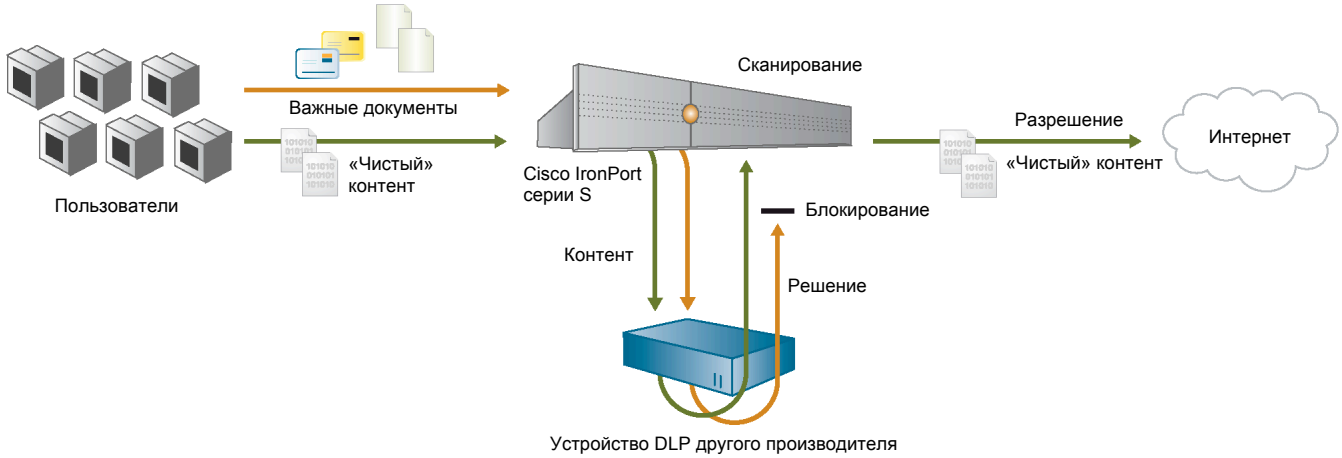
РЕШЕНИЕ CISCO IRONPORT ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ WEB-ТРАФИКА ДАННЫХ (ПРОДОЛЖЕНИЕ)

Устройства обеспечения безопасности web-трафика Cisco IronPort позволяют организациям быстро и легко принимать меры для реализации простых, разумных политик безопасности данных. В качестве примера можно привести запрет инженерам отправлять файлы проектов по открытой электронной почте, блокирование загрузки электронных таблиц размером более 100 кбайт для персонала финансовой службы или предотвращение публикации содержимого в блогах и на сайтах социальных сетей. Эти простые политики безопасности данных можно создать для исходящего трафика протоколов HTTP, HTTPS и FTP.



Разумные политики безопасности данных легко подключаются и реализуются с помощью устройства обеспечения безопасности web-трафика Cisco IronPort.

Для предприятий, которые уже произвели инвестиции в специализированные системы предотвращения потери данных (DLP), устройства обеспечения безопасности web-трафика Cisco IronPort предлагают вариант взаимодействия с поставщиками решений DLP по протоколу ICAP. За счет перенаправления всего исходящего трафика HTTP, HTTPS и FTP на стороннее устройство DLP организации смогут разрешать или блокировать трафик на основании сторонних правил и политик. Это также позволяет выполнять глубокий анализ контента для обеспечения соответствия нормативным требованиям и защиты интеллектуальной собственности, определения степени важности инцидентов, управления инцидентами и оптимизации производительности.



Глубокий анализ контента для трафика HTTP, HTTPS и FTP становится возможным за счет интеграции с устройством DLP другого производителя.

ОПРЕДЕЛЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ ДАННЫХ

Благодаря устройствам обеспечения безопасности web-трафика Cisco IronPort определение политик становится интуитивно понятным и мощным за счет того, что предлагается контроль над конкретными пользователями, группами, объектами, метаданными, репутацией web-узлов, категориями URL-адресов и приложениями (открытой электронной почтой, социальными сетями и т. д.). Эта высокопроизводительная система делает защиту данных интегрированной и прозрачной.

Приложение Cisco IronPort Web Security Manager, поддерживающее создание детализированных политик, позволяет администраторам формировать политики на уровне отдельных пользователей и групп пользователей и в дальнейшем управлять этими политиками, что обеспечивает высочайшую гибкость и управляемость. Кроме того, администраторы имеют возможность определять группы на основе сегментов сети, IP-адресов, подсетей или диапазонов CIDR. Они также могут объединять несколько сегментов сети или отдельных групп в единый блок.

ОПРЕДЕЛЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ ДАННЫХ (ПРОДОЛЖЕНИЕ)

Комплексная фильтрация приложений, объектов и протоколов обеспечивает настройку средств детализированного контроля. Администраторы имеют возможность блокировать или разрешать передачу конфиденциальных данных для любого приложения, использующего протокол HTTP или FTP. Фильтрация объектов (на основании «истинного типа») точно распознает объекты с запретом загрузок, представляющих риск для безопасности и (или) соответствия нормативным требованиям. Устройства обеспечения безопасности web-трафика Cisco IronPort также поддерживают страницы предупреждения/продолжения, позволяющие организациям обучать пользователей корпоративным принципам допустимого использования и политикам безопасности.

Настраиваемые и локализуемые уведомления автоматически сообщают конечным пользователям о нарушении политик в процессе просмотра ресурсов Интернета и передачи данных. Администраторы имеют возможность определить в системе уведомления, которые формируются по более чем 25 инициирующим событиям, либо задать перенаправление на отдельную настраиваемую страницу внутренних политик и уведомлений. Функция настраиваемых уведомлений позволяет администраторам максимально повысить обучающий эффект блокирования web-контента.

ВАРИАНТЫ РАЗВЕРТЫВАНИЯ

Определение масштаба решения для управления безопасностью web-трафика

Линейка продуктов для обеспечения безопасности web-трафика Cisco IronPort предназначена для решения проблем, которые встают перед организациями самых разных размеров – от малого бизнеса до компаний, входящих в список 2000 крупнейших публичных компаний мира по версии журнала Forbes.

Cisco IronPort s670	Предлагается для организаций с числом пользователей более 10 000.
Cisco IronPort s370	Рекомендуется для организаций с числом пользователей от 1000 до 10 000.
Cisco IronPort s170	Предназначен для малого бизнеса и организаций с числом пользователей менее 1000.

ИТОГИ

Cisco предоставляет высокопроизводительные средства комплексного предотвращения потери данных через Интернет, помогая организациям любого масштаба исключить утечку информации, гарантировать соответствие нормативным требованиям и защитить свой брэнд и деловую репутацию. Cisco полагает, что единое решение для мониторинга и обеспечения безопасности данных при их передаче данных по всем коммуникационным каналам, включая Интернет, является жизненно важным для поддержания целостности корпоративных политик. Лидерство на рынке интернет-безопасности в сочетании с партнерскими взаимоотношениями с ведущими в отрасли поставщиками средств DLP ставит Cisco в уникальное положение, позволяющее предлагать простое и удобное в развертывании решение, обладающее этой критически важной функциональностью.

КОНТАКТЫ

Первые шаги

Торговые представители Cisco, партнеры и системные инженеры готовы помощь вам оценить потенциальный вклад продуктов Cisco IronPort в безопасность, надежность и управляемость инфраструктуры вашей корпоративной сети. Если вы сочтете, что ваша организация могла бы воспользоваться преимуществами этих лидирующих в отрасли продуктов, обращайтесь в Cisco представительство.

Cisco
Россия, 115054, Москва,
Космодамианская наб.,
52, стр.1, 4 этаж
Телефон: +7 495 9611410
Факс: +7 495 9611410
www.cisco.ru
www.cisco.com

Cisco
Россия, 197198,
Санкт-Петербург,
пр. Добролюбова, 16, лит. А, кор. 2
Телефон: +7 812 3136230
Факс: +7 812 3136280
www.cisco.ru
www.cisco.com

Cisco
Украина, 03038,
Киев,
ул.Николая Гринчинко, 4В
Тел: +38 044 3913600
Факс: +38 044 3913601
www.cisco.ru
www.cisco.com

Cisco
Казахстан, 050059, Алматы,
Ул. О. Жолдасбекова, 97,
блок А2, 14 этаж
Телефон: +7 727 2442101
Факс: +7 727 244 2102
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)