Средства контроля использования Интернета Cisco IronPort Web Usage Controls

Передовые технологии и наиболее эффективное осуществление политик допустимого использования Интернета

Непредусмотренное использование Интернет каждый год обходится компаниям в миллиарды долларов за счет снижения производительности труда и неэффективного использования ресурсов. Кроме того, при этом появляется вероятность нарушения нормативных требований, ведущая к ответственности перед законом. Эффективность традиционных подходов к решению этой проблемы – использование статических списков URL-адресов, разбитых по категориям – заметно снизилась в условиях динамично развивающейся сети Интернет и все более широкого распространения таких платформ для веб-приложений как Facebook, поскольку эти платформы позволяют использовать множество приложений на одном веб-сайте. Каждый день добавляется более одного миллиарда новых веб-страниц. Благодаря одной только сети Facebook каждый день добавляются сотни новых веб-приложений, что свидетельствует об ошеломляющем успехе Web 2.0 и растущей популярности контента, создаваемого пользователями. Такой взрывной рост объемов контента в сочетании с его быстрым перемешиванием и распространением – более 30% доменов претерпевают ежегодные изменения – привел к созданию «темного web» (dark web), где более 80% содержимого не удается отнести ни к одной категории при использовании разработанных ранее решений. Существование этого «темного Web» подвергает организации тем же самым рискам и заставляет нести те же расходы, которые предполагалось исключить с помощью фильтрации по URL-адресам.

Средства контроля использования Интернет в составе Cisco IronPort, которые есть во всех системах защиты от Интернет-угроз Cisco IronPort серии S, обеспечивают наибольшую в отрасли прозрачность и наилучшую защиту от несанкционированных действий во всемирной сети благодаря сочетанию фильтрации URL-адресов на основе списков, динамической категоризации в режиме реального времени и контролю веб-приложений. В основе этого уникального решения лежит система Cisco Security Intelligence Operations (SIO), которая использует возможности по просмотру трафика в Интернет и делает анализ, позволяющий оценить необходимые усилия для категоризации и обеспечить своевременное обновление для повышения действенности списков URL-адресов.

Сама по себе фильтрация URL-адресов на основе списков не в состоянии решить проблемы, связанные с «теневым web». Средства контроля использования web в составе Cisco IronPort обеспечивают детализированный контроль над встроенными веб-приложениями и динамический анализ содержимого, что приводит к категоризации до 90% нежелательного содержимого, относящегося к «теневому web». В результате увеличение количества обычно блокируемых веб-сайтов может достигать 50%.

Отличительные особенности Cisco IronPort

Продукты Cisco IronPort, предназначенные для работы с электронной почтой и обеспечения веб-безопасности, представляют собой высокопроизводительные, простые в применении и инновационные с технической точки зрения решения, которые призваны обеспечивать безопасность организаций любых размеров. Эти продукты, специально разработанные для обеспечения безопасности и устанавливаемые на уровне шлюза для защиты самых важных в мире сетей, позволяют создать мощную защиту периметра. В системах защиты Cisco IronPort эффективно используется интеллектуальная технология и технология установления глобальной корреляции угроз, заложенная в Cisco SIO, что помогает организациям совершенствовать системы безопасности и прозрачным образом защищать пользователей от новейших Интернет-угроз.

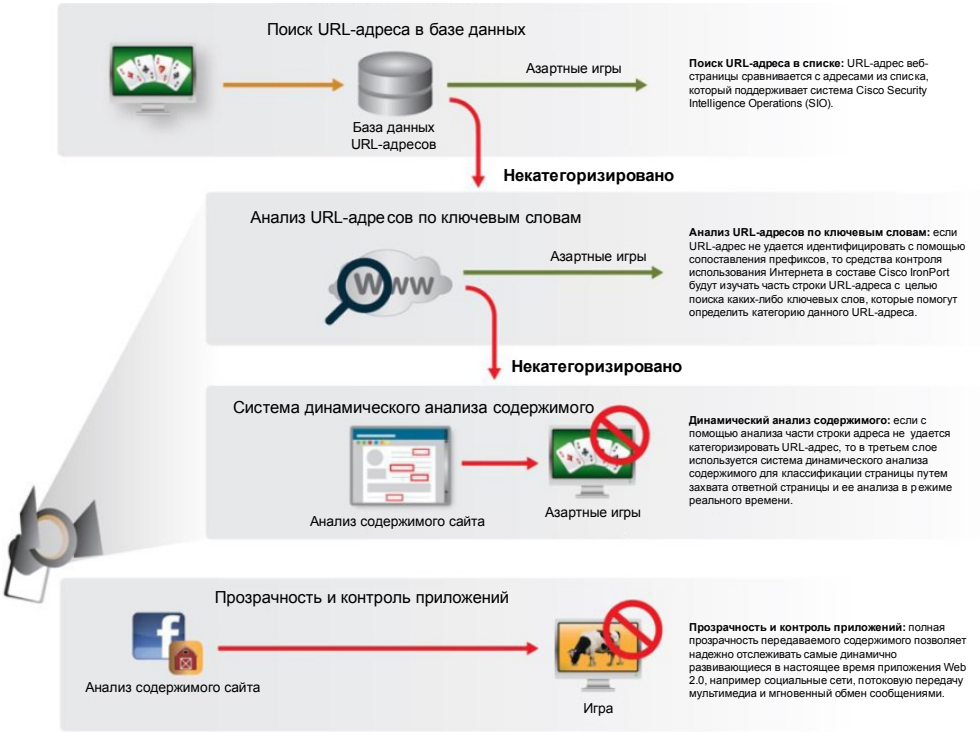
Возможности

Передовые технологии, обеспечивающие эффективность

Средства контроля использования Интернета в составе Cisco IronPort используют несколько слоев для категоризации URL-адресов, что позволяет получить высочайший уровень эффективности и наибольший охват сети Интернет, включая «теневой Web». В решении предусмотрено 65 категорий URL-адресов и полная база URL-адресов, охватывающая веб-сайты более чем в 200 странах на более чем 50 языках.

Расширяемая архитектура, способная контролировать тысячи приложений, обновляется в динамическом режиме по мере изменения приложений или добавления новых приложений.

© Cisco и/или ее дочерние компании, 2012. С сохранением всех прав. В данном документе содержится общедоступная информация Cisco.



Система Cisco SIO обновляет базу данных каждые пять минут, благодаря возможности отслеживать более трети глобального Интернет-трафика, и это обеспечивает клиентам самое эффективное и своевременное покрытие Интернета. Обновление сигнатур приложений происходит в динамическом режиме, что обеспечивает эффективность и поддержку для новых приложений, которые должны развертываться независимо от циклов выпуска платформы. Обновление URL-адресов выполняется благодаря применению технологий автоматического изучения и классификации веб-сайтов в сочетании с проводимой вручную классификацией, которой занимаются профессиональные исследователи из группы глобальной категоризации Cisco. Регулярно автоматически выбраковываются неиспользуемые домены и веб-сайты, также регулярно производится обновление с учетом миллионов новых URL-адресов, что позволяет поддерживать самое высокое в отрасли качество базы данных для фильтрации веб-сайтов.

Помимо этого, данные от тысяч систем защиты от Интернет-угроз Cisco IronPort серии S (которые развернуты по всему миру) стекаются в систему Cisco SIO для классификации некатегоризированных URL-адресов. Это позволяет быстро, буквально через несколько минут, получить ответ на любые запросы, связанные с невозможностью категоризации.

Обзор и контроль приложений

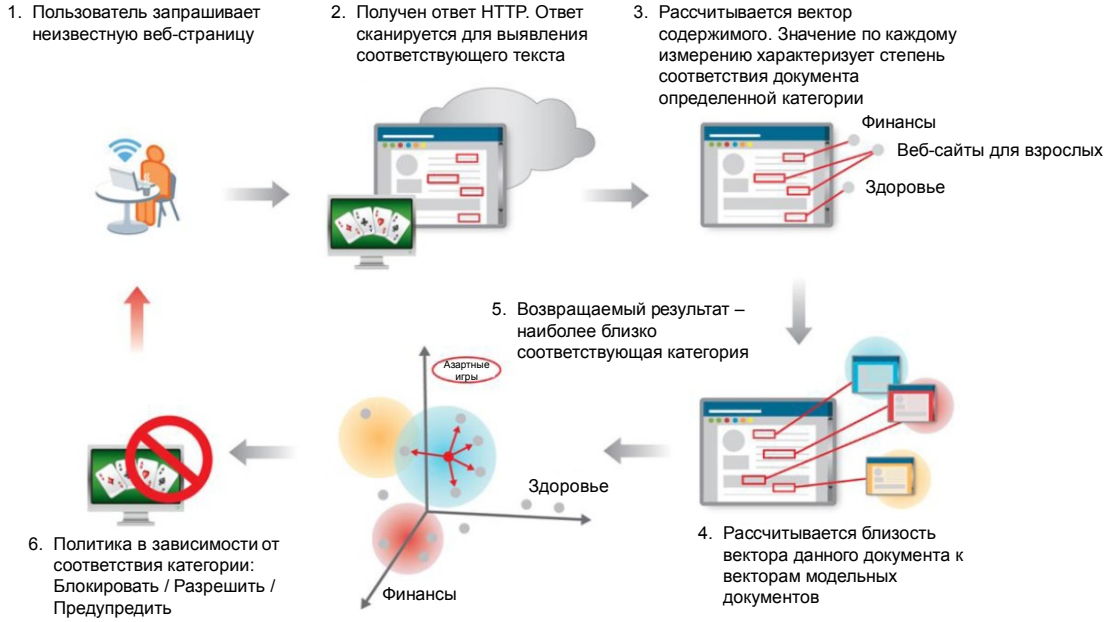
Обзор приложений и возможности контроля, заложенные в Cisco IronPort, обеспечивают детализированный контроль множества типов встроенных приложений, которые могут существовать на одной веб-странице. В результате организации могут разрешать доступ к веб-сайтам, сохраняя контроль за этим процессом. Динамические сигнатуры приложений позволяют идентифицировать отдельные действия в рамках приложения, например чат в приложении Facebook или обновление статуса. В рамках пользовательского интерфейса можно легко определить политику по каждому элементу вплоть до уровня пользователя.

Способность контролировать потоковую передачу мультимедиа дает организациям еще большие возможности управления встроенным видео-контентом и контроля веб-сайтов с высокой пропускной способностью. Это достигается благодаря разрешениям на использование мультимедиа, связанного с деятельностью организации, и установлению ограничений для прочего видео-контента.

© Cisco и/или ее дочерние компании, 2012. С сохранением всех прав. В данном документе содержится общедоступная информация Cisco.

Динамическая категоризация, проводимая локально в режиме реального времени

Система динамического анализа содержимого оценивает все некатегоризированное веб-содержимое – даже то, что скрыто в SSL-туннеле – для принятия решений о категоризации в режиме реального времени. Для расчета концептуального вектора используются современные эвристические методы, после чего полученный вектор сравнивается с обширной библиотекой модельных документов для быстрого и точного определения категории содержимого. Система настроена на максимальную скорость захвата нежелательного содержимого, которое обычно блокируется, что снижает для клиентов вероятность нарушения законодательных и нормативных требований, сохраняя на низком уровне количество ошибочных положительных заключений.



Широкий набор элементов управления политиками и комплексная отчетность

Средства контроля использования Интернета в составе Cisco IronPort обладают богатыми возможностями контроля доступа к Интернету. Предусмотрены такие возможности как «Блокировать», «Разрешить», «Предупредить» и «Отслеживать», а также контроль в зависимости от времени дня. Интеграция с существующей службой каталогов Active Directory или с Lightweight Directory Access Protocol (LDAP) позволяет осуществлять политики на уровне пользователя и группы пользователей. Настраиваемые категории с поддержкой регулярных выражений обеспечивают гибкость при создании практически неограниченного количества создаваемых пользователем белых и черных списков.

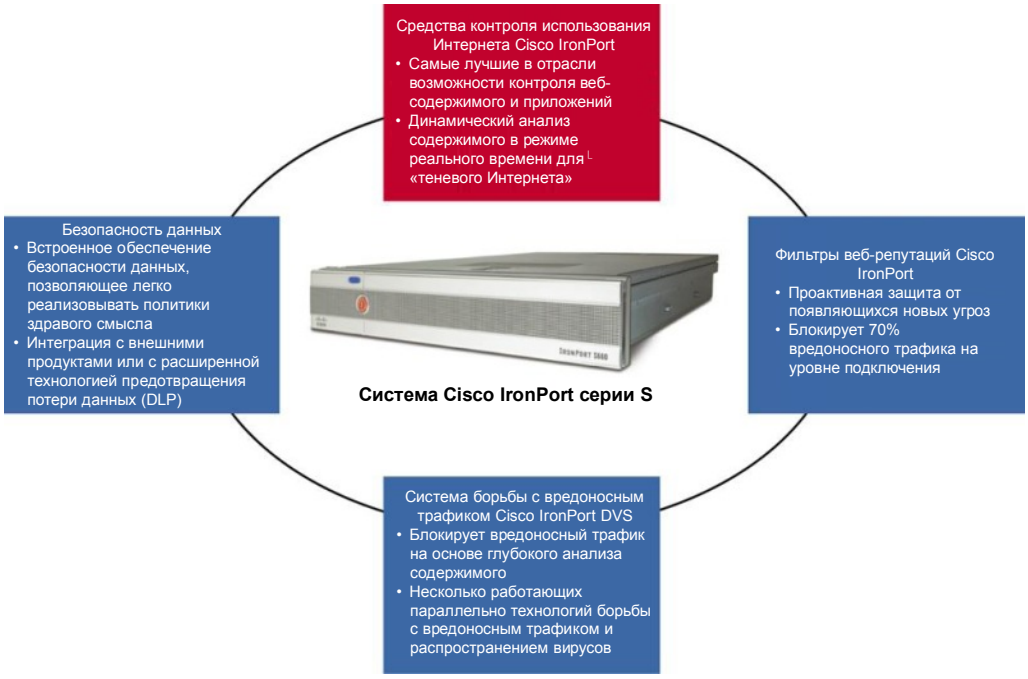
Решение позволяет создавать комплексные отчеты, которые могут быть как внешними, так и локальными. Отчеты являются полностью интерактивными, что позволяет администратору начать с просмотра сводок верхнего уровня, например узнать количество пользователей, заблокированных политикой. С помощью одного нажатия клавиши администратор может увидеть, какие политики сработали или кто из пользователей был наиболее серьезно заблокирован. Нажав клавишу еще раз, администратор сможет увидеть весь трафик конкретного пользователя, действия которого нарушили ту или иную политику.

Такая система отчетности позволяет администраторам быстро выявлять проблемы, а затем либо корректировать политику, либо принимать другие подходящие меры. Журналы можно экспортировать для дальнейшего анализа и принятия решений. В этом решении также предусмотрена комплексная система оповещений при использовании поддержки корпоративного класса.

Полностью интегрированная веб-безопасность

Средства контроля использования Интернета в составе Cisco IronPort полностью интегрированы в систему защиты от Интернет-угроз Cisco IronPort серии S, которая является первым в отрасли и единственным безопасным веб-шлюзом, сочетающим в одной платформе традиционный способ фильтрации URL-адресов, репутационную фильтрацию и защиту от вредоносных программ, а также обеспечение безопасности данных.

© Cisco и/или ее дочерние компании, 2012. С сохранением всех прав. В данном документе содержится общедоступная информация Cisco.



Категории фильтрации URL-адресов

Средства контроля использования Интернета в составе Cisco IronPort предусматривают 65 категорий URL-адресов и охват веб-сайтов более чем в 200 странах на более чем 50 языках. Категории URL-адресов:

Веб-сайты для взрослых
Реклама
Алкоголь и табак
Искусство и развлечения
Бизнес и промышленность
Обман и плагиат
Детская порнография
Компьютерная безопасность
Компьютеры и Интернет
Культы
Знакомства
Еда и напитки
Образование
Службы передачи файлов
Приемы, позволяющие избежать фильтрацию
Финансы
Бесплатное и условно-бесплатное программное обеспечение
Азартные игры
Игры
Правительство и закон
Неавторизованный доступ
Пропаганда вражды и ненависти
Здоровье и питание
Незаконные действия
Незаконный оборот наркотиков
Инфраструктура
Обмен мгновенными сообщениями
Интернет-телефония
Поиск работы
Белье и купальники
Лотерея и тотализатор
Мобильные телефоны
Природа
Новости
Несексуальное обнажение тела
Сетевые сообщества
Хранение и архивирование данных в сети
Интернет-торговля
Паранормальные явления и оккультизм
Передача файлов в локальной сети
Порнография
Недвижимость
Справки
Безопасные продукты для детей
Наука и технология
Системы поиска и порталы
Половое воспитание и аборты
Шоппинг
Социальные сети
Социология
Общество и культура
Обновление программного обеспечения
Психотерапия
Спорт и отдых
Потоковая передача мультимедиа
Дурной вкус или непристойности
Татуировки
Перевозки
Путешествия
Жестокость и насилие
Оружие
Веб-хостинг
Перевод веб-страниц
Интернет-чат
Интернет-почта

© Cisco и/или ее дочерние компании, 2012. С сохранением всех прав. В данном документе содержится общедоступная информация Cisco.

Заключение

Средства контроля использования Интернета в составе Cisco IronPort представляют собой передовое решение для реализации политик контроля допустимого использования сети Интернет. Улучшенные возможности контроля веб-трафика и веб-приложений повышают производительность труда персонала компаний. В этом эффективном решении реализовано сочетание самой точной базы данных URL-адресов с самым широким в отрасли покрытием и динамической категоризацией в режиме реального времени для выявления нежелательного веб-содержимого. Предусмотрено динамическое обновление контроля приложений, что позволяет охватывать новые приложения и сохранять контроль при изменении существующих приложений.

Данное решение поддерживается системой Cisco SIO, которая имеет беспрецедентные возможности контроля трафика в глобальной сети, обеспечивая постоянное обновление соответствующих адресов в базе данных URL-адресов и сигнатур приложений. Средства контроля использования Интернета в составе Cisco IronPort отличаются широкими возможностями контроля с учетом политик и создания комплексных отчетов. Эти средства контроля интегрированы в систему Cisco IronPort серии S, что создает целостное и безопасное решение – веб-шлюз, в котором предусмотрена защита от вредоносных программ, широкий набор средств контроля допустимого использования Интернета и безопасность данных.

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)