ПЕРСОНАЛИЗИРОВАННЫЕ УСЛУГИ БЕЗОПАСНОСТИ ДЛЯ АБОНЕНТОВ ШИРОКОПОЛОСНОГО ДОСТУПА В ИНТЕРНЕТ

В последние годы наблюдается бурный рост числа разнообразных угроз информационной безопасности в сети Интернет. В этой ситуации, на операторов связи ложиться задача по обеспечению эффективной защиты от вирусов, зомби-сетей, распределенных атак типа "отказ в обслуживании" (DDoS-атак), рассылок спама и Интернет-мошенничества (фишинга). Решения компании Cisco Systems по обеспечению сетевой безопасности защищают от такого рода угроз более эффективно, чем неконтролируемые оператором связи программные средства защиты персональных компьютеров абонентов, которые зачастую неправильно внедряются и нерегулярно обновляются абонентами. Операторские сервисы по информационной безопасности позволяют обеспечить защиту абонентов, учитывая такие особенности как тип доступа и фактические потоки трафика каждого абонента. Средства самообслуживания позволяют оперативно оповещать абонентов о появлении вредоносных программ и предоставляют возможность абонентам самостоятельно защитить свои компьютеры. Различные сервисы по обеспечению информационной безопасности, предоставляемые абонентам сетей широкополосного доступа, объединены под названием "Персонализированные Услуги Безопасности".

В данном документе рассматриваются технологии и решения, обеспечивающие защиту при подключении к широкополосным сетям доступа в Интернет, входящие в состав персонализированных услуг безопасности, в том числе ядро управления услугами (Cisco Service Control Engine - SCE) и интеллектуальный шлюз услуг (Cisco Intelligent Services Gateway - ISG).

ОБЗОР

Абоненты все чаще полагаются на операторов связи в вопросах защиты от вирусов, спама и прочих Интернет-угроз. Незащищенные компьютеры миллионов, ничего не подозревающих, абонентов могут оказаться зараженными вредоносным ПО в результате чего, они контролируются злоумышленниками и становиться инструментами рассылки спама и запуска DDoS-атак.

Предлагаемые компанией Cisco Systems технологии и продукты позволяют оператору связи и абоненту принять непосредственное участие в обеспечении безопасности, как индивидуальных активов абонента, так и широкополосной сети оператора в целом. В этих условиях операторы связи имеют возможность развивать спектр предлагаемых услуг и получать дополнительные доходы за счет развертывания персонализированных средств защиты. Эти средства предоставляют абонентам возможность самостоятельного выбора различных параметров защиты и позволяют эффективно противостоять угрозам безопасности. Таким образом, абоненты могут сами контролировать безопасность своего подключения к сети, что позволяет существенно снизить нагрузку на центр обработки вызовов оператора связи.

Для организации персонализированных услуг безопасности применяются современные решения Cisco Systems, позволяющие анализировать и контролировать различные характеристики трафика приложений, используемых каждым абонентом, что дает возможность обеспечить полное управление

приложениями в рамках каждой услуги. Это позволяет защитить пользователей широкополосной сети от DDoS-атак, распространения вирусов и других угроз, а также дать операторам связи возможность предоставлять надежные персонализированные услуги самообслуживания.
Эти услуги предусматривают возможность персональной настройки из "личного кабинета" абонента, а также позволяют использовать в работе средства классификации контента и ограничения доступа (включая системы родительского контроля), средства фильтрации спама и контроля его источников и средства защиты от DDoS-атак, червей, вирусов, атак сканирования и других угроз.

ЗАДАЧИ

Миллионы пользователей во всем мире испытывают проблемы от увеличения объемов спама, распространения вредоносного ПО и роста кибер-преступности. Проведенное в 2006 году исследование издания "Consumer Reports" показало, что с помощью фишинговых атак в Соединенных Штатах в 2005 году было похищено 630 миллионов долларов, а в 2006 году общая стоимость потерь от вирусов, шпионских программ и фишинга только в Соединенных Штатах составила свыше 8 миллиардов долларов. С января 2005 года по март 2006 года 270 миллионов пользователей, использовавших бесплатное средство сканирования ПК компании Microsoft, обнаружили вредоносный код на 5,7 млн компьютеров, среди которых было 3,5 млн зомби-компьютеров, контролируемых злоумышленниками через защищенный канал обмена сообщениями.
По оценкам компании Trend Micro около 100 миллионов компьютеров по всему миру являются зомби-компьютерами, причем 15 миллионов из них активны в разное время суток. В ноябре 2006 года агентство "Рейтер" сообщило, что "Великобританию захлестнула волна нежелательных сообщений электронной почты на тему секса, наркотиков и рекламы, распространяемых криминальными структурами с зараженных компьютеров". По оценкам компании Postini, занимающейся обеспечением безопасности электронной почты, объем спама за период с ноября по июнь 2006 года вырос втрое, и в настоящее время спамом являются девять из десяти передаваемых сообщений электронной почты.
Абоненты широкополосных сетей хотят получать дополнительные услуги по обеспечению информационной безопасности и согласны платить за них. Проведенное в 2004 году исследование компании Jupiter Research показало, что 47 процентов пострадавших абонентов широкополосных сетей согласны платить за дополнительный пакет услуг (value-added service - VAS), который должен включать услуги по обеспечению безопасности. Через год аналогичное исследование компании Ipsos-Mori показало, что это число возросло до 58 процентов. Кроме того, были получены следующие данные:

- 54 процента абонентов согласны на увеличение ежемесячной платы за доступ Интернет более чем на 3 доллара при условии предоставления безопасных Интернет-услуг.
- 66 процентов абонентов заявили о намерении поменять оператора связи, если другой оператор сможет обеспечить лучшую защиту.

В условиях высокой конкуренции и изменяющегося рынка операторам связи приходится искать способы выделить свои услуги по сравнению с услугами

конкурентов. В то же время операторы связи обязаны защищать отдельных клиентов и широкополосные сети в условиях быстрого роста объемов сетевого трафика и наличия как защищенных, так и незащищенных компьютеров абонентов. Наличие эффективных средств обеспечения безопасности является конкурентным преимуществом, позволяющим сократить отток клиентов, повысить степень удовлетворенности заказчиков, стимулировать потребление других сетевых услуг и повысить рейтинг оператора связи за счет рекомендаций клиентов, удовлетворенных уровнем сервиса.

РЕШЕНИЕ

Персонализированные услуги безопасности - это решения, целиком реализованные в сетевой инфраструктуре оператора связи. Услуги по персонализированной защите абонентов одновременно обеспечивают и защиту самих широкополосных сетей. Они не требуют наличия агентов на стороне абонента (например, установки специального ПО для обеспечения безопасности). Услуги реализуются на базе сети оператора связи и специальных средств управления и обеспечения информационной безопасности.

На рисунке 1 "Решения Cisco Systems по обеспечению безопасности широкополосных сетей" показаны составляющие системы безопасности широкополосного доступа. Этот уникальный всеобъемлющий подход к безопасности сети позволяет одновременно использовать преимущества высококачественных услуг широкополосного доступа и предложить персонализированные услуги по обеспечению безопасности для абонентов широкополосной сети.

Рисунок 1. *Компоненты решения Cisco по обеспечению безопасности широкополосной сети.*

В состав решения Cisco Systems по обеспечению безопасности широкополосного доступа входят следующие компоненты:

- **Архитектура нового поколения IP-сетей операторов связи** (IP Next Generation Network; IP NGN). Эта архитектура широкополосной сети позволяет обеспечить мониторинг и контроль за возможными угрозами ИБ, возникающими в широкополосных сетях.
- **Управляемые сервисы для заказчиков**. На основе защищенной широкополосной сети с использованием оборудования Cisco Systems операторы связи имеют возможность оказывать дополнительные услуги по обеспечению информационной безопасности для корпоративных клиентов и управлять этими услугами, получая при этом значительную прибыль.
- **Персонализированные услуги безопасности**. Эти услуги позволяют снизить объемы спама, защитить абонентов широкополосного доступа от вирусов и червей, обеспечить защиту абонентов от фишинговых-атак и предоставить абонентам возможность самостоятельно отслеживать, контролировать и ограничивать доступ к определенным ресурсам в сети Интернет.

ПРОДУКТЫ И ТЕХНОЛОГИИ, ПОЗВОЛЯЮЩИЕ РЕАЛИЗОВАТЬ "ПЕРСОНАЛИЗИРОВАННЫЕ УСЛУГИ БЕЗОПАСНОСТИ"

Персонализированные услуги безопасности используют технологии, развертываемые внутри инфраструктуры управления сервисами (Cisco Service Exchange Framework - Cisco SEF) (рисунок 2), которая является уровнем создания и управления сервисами в рамках архитектуры Cisco IP NGN. Решения Cisco Systems для обеспечения информационной безопасности интегрированные в архитектуру самозащищающейся сети Cisco (Cisco Self-Defending Network) позволяют добиться максимального уровня безопасности без приобретения конечными пользователями дополнительного оборудования.

Рисунок 2. *Инфраструктура обмена услугами Cisco Service Exchange Framework*

К решениям, обеспечивающим безопасность широкополосного доступа, включая Персонализированные Услуги Безопасности, относятся: маршрутизаторы и коммутаторы уровней доступа, агрегации и ядра, а так же различные сервисы по обеспечению безопасности. Внутри инфраструктуры Cisco SEF развертываются два продукта, позволяющие обеспечить беспрецедентный уровень безопасности:

- **Устройство Cisco Service Control Engine** (Cisco SCE) обнаруживает трафик определенных приложений конкретного абонента и управляет им в реальном времени. Этот продукт классифицирует трафик и исследует работу приложений, а затем направляет трафик на дополнительные серверы услуг информационной безопасности для тщательной проверки, что позволяет значительно расширить анализ с целью обеспечения безопасности. Эта возможность значительно повышает уровень безопасности для каждого отдельного абонента.
- **Сервис Cisco Intelligent Services Gateway** (Cisco ISG), доступный в маршрутизаторах Cisco Systems, автоматически фиксирует попытки доступа абонентов в сеть и определяет тип услуги, которая необходима каждому абоненту, а также тип используемого устройства. Cisco ISG способен управлять доступом к услугам разного типа - как мультимедийным подсистемам, так и другим услугам, в том числе не использующим протокол SIP (Session Initiation Protocol).

С целью повышения степени защиты наряду с указанными продуктами и технологиями Cisco Systems можно использовать решения сторонних производителей по обеспечению безопасности. Предполагается непрерывное развитие описанных в этом документе Персонализированных Услуг Безопасности с целью противостояния новым угрозам и методам вторжения.

СОСТАВ ПЕРСОНАЛИЗИРОВАННЫХ УСЛУГ БЕЗОПАСНОСТИ

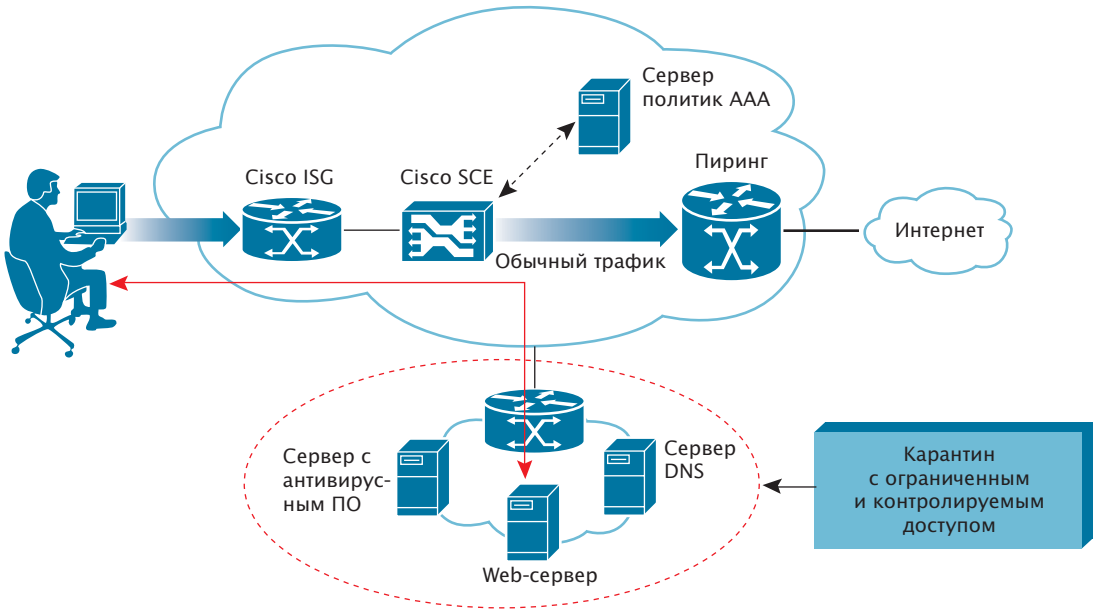
Развертывая описанные ниже продукты и технологии, операторы связи получают возможность предоставлять широкий спектр весьма прибыльных персонализированных услуг безопасности. Эти персонализированные услуги дают абонентам возможность получить беспрецедентный контроль над безопасностью собственного доступа, повышая тем самым уровень защиты широкополосных сетей в целом. Такой уровень безопасности позволяет сэкономить время и деньги как абонентам, так и операторам связи.

- Центр самообслуживания. Если компьютер абонента заражен вредоносным ПО, попавшим в широкополосную сеть, то такой абонент перенаправляется на web-страницу центра самообслуживания с целью предотвращения распространения вредоносного ПО (рисунок 3). В центре самообслуживания абоненту предлагаются возможные средства устранения проблемы. Применение этой услуги всеми абонентами позволяет в целом защитить широкополосные сети операторов связи.

  Принцип работы. Cisco SCE распознает потенциальные угрозы безопасности путем анализа всего трафика абонента с помощью эвристических методов и методов анализа поведения. Cisco SCE работает непосредственно с трафиком, обращаясь при необходимости к дополнительным серверам услуг

ИБ и используя их как средства фильтрации. При обнаружении в сетевом трафике признаков заражения компьютера абонента Cisco SCE может заблокировать подозрительный трафик абонента или уведомить абонента о сложившейся ситуации, перенаправив его на web-страницу центра самообслуживания. После завершения проверки и удаления вредоносного ПО с компьютера абонента, ему предоставляется прежний вид доступа в сеть.

Рисунок 3. *Центр самообслуживания*

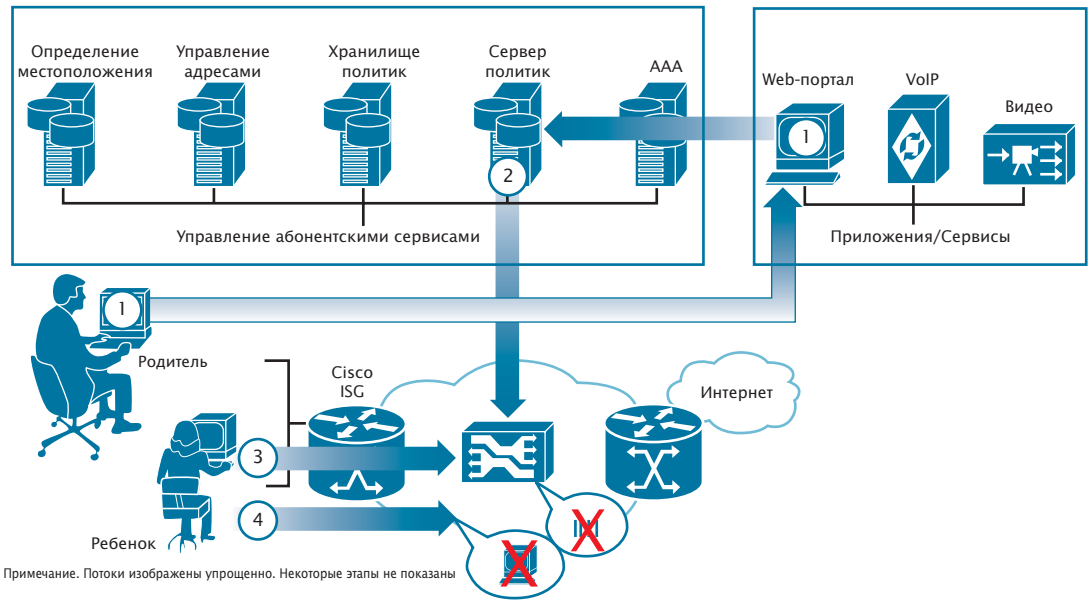


- **Классификация контента и ограничение доступа к определенным ресурсам сети Интернет.** Родители могут классифицировать Интернет-контент, накладывать ограничения на его использование, а также устанавливать ограничения по времени просмотра с тем, чтобы оградить детей от неподобающего или нежелательного содержимого. На web-портале родители могут настроить параметры, определяющие правила использования Интернета детьми (рисунок 4). С помощью этих параметров можно определить ограничения по времени (например, разрешить доступ только в течение двух часов по понедельникам, средам и пятницам) или запретить доступ младших членов семьи к некоторым web-сайтам с домашнего компьютера. Руководство организаций так же может ограничивать доступ сотрудников к вредному или нежелательному содержимому. Операторы связи могут предоставлять отдельную подписку на эту услугу за дополнительную плату.

  Принцип работы. Решение Cisco SCE позволяет осуществлять классификацию http-запросов в соответствии со списком URL-адресов в реальном времени без какого-либо заметного снижения производительности сети. Cisco SCE может хранить список, включающий до 100 000 URL-адресов. После того как родитель или другой абонент определил настройки для учетных записей, соответствующих другим пользователям, Cisco SCE перехватывает пакеты, исходящие из домашнего компьютера, и выполняет управление

доступом к URL-адресу за счет использования внутреннего кэша URL-адресов, обновляемого из общих хранилищ URL-адресов, с учетом настроек фильтрации. Кроме того, Cisco SCE может взаимодействовать с системами родительского контроля сторонних производителей, запрашивая классификацию URL-адресов и применяя соответствующую политику для конкретного абонента.

Рисунок 4. *Самостоятельная классификация контента и ограничение доступа*

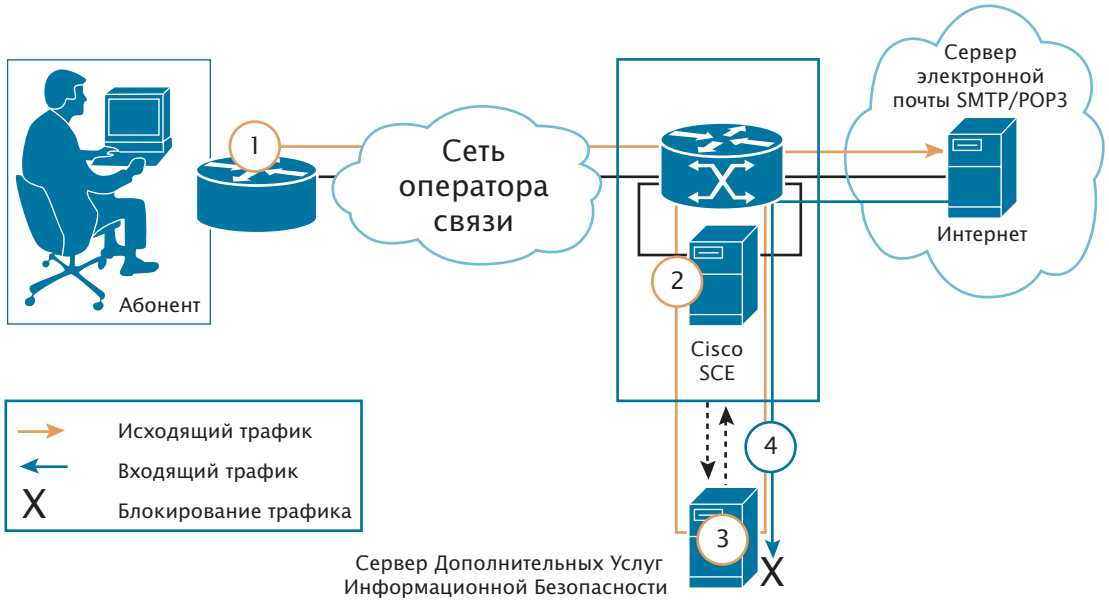


1 Пользователь заходит на Web-портал и выбирает приложения, сетевой доступ к которым необходимо предоставить для различных учетных записей, а также временные ограничения по их использованию. Пользователь также указывает web-сайты, доступ к которым необходимо ограничить.
2. Сервер политик загружает заданными родителем настройки на Cisco SCE.
3. Ребенок пытается использовать программу обмена сообщениями и обнаруживает, что эта услуга заблокирована с 23:00 до 7:00
4. Ребенок пытается открыть запрещенную web-страницу и обнаруживает, что доступ к этой странице заблокирован.

- **Фильтрация спама и контроль его источников.** Интеллектуальные решения Cisco Systems способны обнаруживать и блокировать распространение спама как исходящего от абонентов, так и поступающего к абонентам. Операторы связи могут предоставлять отдельную подписку на эту услугу за дополнительную плату.

  Принцип работы. В рамках данного решения Cisco SCE используется для перенаправления почтового трафика SMTP на сервер дополнительных услуг ИБ для выполнения проверки (рисунок 5). Помимо этого, устройство Cisco SCE способно распознавать зараженные компьютеры ничего не подозревающих абонентов, которые используются для рассылки спама. Cisco SCE подсчитывает число исходящих SMTP-сессий и сравнивает его с предварительно заданным пороговым значением. В случае резкого роста количества SMTP-сессий, исходящих с компьютера какого-либо абонента, оператору связи направляется соответствующее уведомление. Cisco SCE может заблокировать подозрительный трафик или уведомить конечного пользователя об обнаруженном нарушении.

Рисунок 5. *Защита абонентов от рассылок спама.*



1. Абонент пытается получить электронную почту с сервера электронной почты в Интернет
2. Cisco SCE определяет, данный абонент подписан на услугу по фильтрации спама.
3. Сервер дополнительных услуг получает трафик от Cisco SCE.
   Почтовый клиент обнаруживает на POP3 сервере несколько новых сообщений.
4. Сервер электронной почты передает очередное сообщение, являющееся спамом
   Сервер дополнительных услуг заблокирует сообщение или отметит его как спам.
   Далее все сообщения пересылаются с сервера дополнительных услуг назад на Cisco SCE, а затем отправляется абоненту.

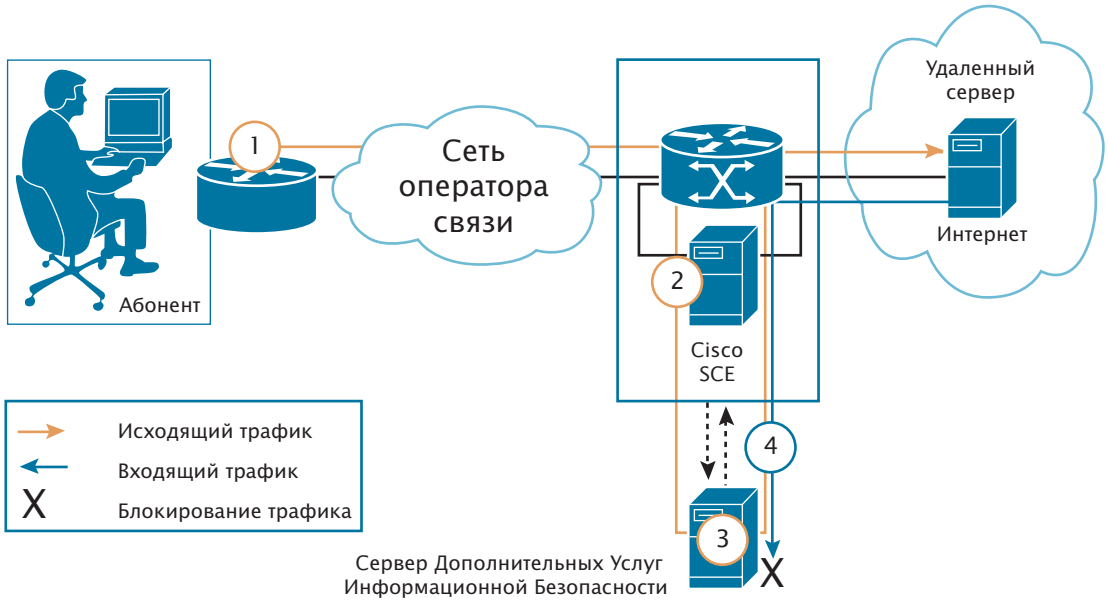
Cisco SCE может также использоваться в качестве предварительного фильтра, который позволяет снизить нагрузку и при необходимости перенаправить трафик электронной почты на более мощное устройство обнаружения спама.

- **Персонализированная защита абонентов.** Интеллектуальные решения Cisco могут взаимодействовать с дополнительными системами обеспечения безопасности сторонних производителей с целью обнаружения и блокирования вредоносного ПО, предотвращения хищения персональных данных, а также вирусных атак на компьютеры абонентов. Операторы связи могут предоставить доступ к бесплатной услуге самообслуживания или бесплатно включить такую услугу в пакет услуг широкополосного доступа для абонентов.

  Принцип работы. Это сетевое решение, в котором Cisco SCE используется в сочетании с системами дополнительных услуг ИБ с целью обнаружения DDoS-атак, червей, сканирования сети и других угроз. Cisco SCE способно переадресовать потоки трафика в зависимости от подписки услуг абонента (рисунок 6). Cisco SCE переадресовывает трафик абонентов на сервер дополнительных услуг ИБ, который может в реальном времени анализировать вложения электронной почты, обнаруживать вредоносный код на web-страницах и в файлах, получаемых по протоколу FTP. Сервер

дополнительных услуг ИБ позволяет обнаружить и заблокировать вирусы и прочее вредоносное ПО и предотвратить заражение персонального компьютера абонента.

Рисунок 6. *Персонализированная защита абонентов*



1. Абонент пытается получить электронную почту с сервера электронной почты или загрузить файл с web-сайта в Интернет.
2. Cisco SCE определяет, что потоки трафика абонента соответствуют подписке на дополнительные сервисы обеспечения ИБ
3. Сервер дополнительных услуг получает трафик от Cisco SCE.
4. Сервер в сети Интернет передает абоненту файл, содержащий вирус или другое вредное ПО. Сервер дополнительных услуг ИБ обнаруживает и блокирует встроенное вредное ПО, тем самым, предотвращая заражение компьютера абонента

Персонализированные Услуги Безопасности позволяют операторам связи:

- Получить конкурентное преимущество за счет расширения спектра предоставляемых услуг;
- Получить новые источники доходов;
- Снизить количество ошибок при определении угроз за счет применения специализированных средств мониторинга сетевого трафика;
- Своевременно и точно идентифицировать появление новых угроз в сети, за счет анализа статистической информации о трафике;
- Обеспечить защиту всех устройств, подключенных через широкополосную сеть;
- Блокировать угрозы безопасности и снизить загрузку широкополосной сети за счет уменьшения объемов нежелательного трафика;
- Снизить риск Интернет-мошенничества за счет блокирования шпионского ПО, фишинга и фарминга.

Использование персонализированных услуг безопасности дает абонентам следующие преимущества:

- Обнаружение и блокирование угроз выполняется в сети, а не на компьютерах

абонентов;
- Работа услуг по защите начинается сразу после оформления пользователем подписки на услугу широкополосного доступа;
- Нет необходимости следить за обновлениями программного обеспечения персональных компьютеров абонентов;
- Нет необходимости устанавливать дополнительное ПО на компьютерах абонентов;
- Абоненту не требуется приобретать дополнительное оборудование для обеспечения ИБ.

ЗАКЛЮЧЕНИЕ

Персонализированные Услуги Безопасности могут помочь операторам связи снизить нагрузку на центры обслуживания клиентов и обеспечить дополнительную защиту своих широкополосных сетей. Множество функций самообслуживания предоставляют возможность абонентам самостоятельно ограничивать доступ к определенному контенту в сети Интернет. Эти услуги по обеспечению безопасности могут использоваться для защиты отдельных абонентов, их семей и широкополосных сетей в целом. За счет применения встроенных интеллектуальных средств обеспечения безопасности на всех уровнях архитектуры Cisco IP NGN и таких систем, как Cisco SCE и Cisco ISG, Персонализированные Услуги Безопасности позволяют операторам связи увеличить лояльность клиентов и получить существенный доход.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Архитектура Cisco IP NGN:
http://www.cisco.com/en/US/netsol/ns537/networking_solutions_announcement0900aecd80381291.html#srvc_conv
Продукты и технологии Cisco для предоставления персонализированных услуг абонентам: http://www.cisco.com/en/US/netsol/ns715/netbr0900aecd8055c187.html
Официальный документ с описанием решений
Cisco по обеспечению безопасности сетей широкополосного доступа:
http://www.cisco.com/en/US/netsol/ns734/networking_solutions_white_papers_list.html
Cisco Intelligent Services Gateway (Cisco ISG):
http://www.cisco.com/en/US/products/ps6588/products_ios_protocol_group_home.html
Cisco SCE 2000 Series Service Control Engine:
http://www.cisco.com/en/US/products/ps6478/index.html
Cisco Broadband Policy Manager: http://www.cisco.com/en/US/products/ps6151/index.html
Cisco Service Exchange: http://www.cisco.com/go/serviceexchange

Cisco
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб.,
52, стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco
Казахстан, 480099,
Алматы,
бизнес-центр «Самал 2»
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: + 7 (3272) 58 46 58
Факс: + 7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco
Украина, 252004, Киев,
бизнес-центр
«Горайзон Парк»
Ул. Николая Гринченко, 4В
Киев, 03038, Украина
Тел.: + 7 (38044) 490 36 00
Факс: + 7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

Cisco
Азербайджан,
AZ 1065, Баку,
бизнес-центр «Карат»
Ул. М. Мухтарова, 201,
этаж 2
Тел.: + 7 (99412) 437 48 20
Факс: + 7 (99412) 437 48 21
www.cisco.ru
www.cisco.com

Cisco
Узбекистан, 100000,
Ташкент, бизнес-центр
«ИНКОНЕЛЬ»
Ул. Пушкина, 75, офис 605,
этаж 6
Тел.: + 7 (99871) 140 44 60
Факс: + 7 (99871) 133 44 64
www.cisco.ru
www.cisco.com

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

Argentina ▪ Australia ▪ Austria ▪ Belgium ▪ Brazil ▪ Bulgaria ▪ Canada ▪ Chile ▪ China PRC ▪ Colombia ▪ Costa Rica ▪ Croatia ▪ Cyprus ▪ Czech Republic ▪ Denmark ▪ Dubai, UAE ▪ Finland ▪ France ▪ Germany ▪ Greece ▪ Hong Kong ▪ SAR ▪ Hungary ▪ India ▪ Indonesia ▪ Ireland ▪ Israel ▪ Italy ▪ Japan ▪ Korea ▪ Luxembourg ▪ Malaysia ▪ Mexico ▪ The Netherlands ▪ New Zealand ▪ Norway ▪ Peru ▪ Philippines ▪ Poland ▪ Portugal ▪ Puerto Rico ▪ Romania ▪ Russia ▪ Saudi Arabia ▪ Scotland ▪ Singapore ▪ Slovakia ▪ Slovenia ▪ South Africa ▪ Spain ▪ Sweden ▪ Switzerland ▪ Taiwan ▪ Thailand ▪ Turkey ▪ Ukraine ▪ United Kingdom ▪ United States ▪ Venezuela ▪ Vietnam ▪ Zimbabwe