Оператор домашних сетей контролирует трафик

Петербуржский оператор домашних сетей «Ниеншанц-Хоум» запустил в эксплуатацию решение компании Cisco Systems по контролю трафика на уровне приложений на базе Cisco Service Control Engine 2020.

КРАТКИЙ ОБЗОР

Компания «Ниеншанц-Хоум»
- Оператор домашних сетей
- Санкт-Петербург, РФ
- Более 20 000 абонентов

БИЗНЕС-ЗАДАЧА
- Увеличение абонентской базы.
- Повышение лояльности абонентов.
- Внедрение дополнительных сервисов.
- Контроль трафика на уровне приложений.
- Повышение доходности.

РЕШЕНИЕ
- Внедрение Cisco Service Control Engine

РЕЗУЛЬТАТЫ
- Оптмизация Интернет трафика.
- Сокращение расходов.
- Внедрение новых сервисов.
- Повышение лояльности абонентов.

Бизнес-задача

В настоящее время перед операторами домашних сетей стоят различные задачи: увеличение абонентской базы и как следствие развитие собственной инфраструктуры, расширение предоставляемых сервисов, повышение лояльности абонентов, минимизация времени простоя и т.д. Все эти задачи в комплексе подобны задачам, стоящим перед традиционными операторами проводной и мобильной связи. Но зачастую, из-за меньших размеров компаний операторов-домашних сетей, эти задачи и вызываемые ими проблемы проявляются ярче и сильнее. При этом современные тенденции показывают, что крупные проводные и мобильные операторы также стремятся выйти на рынок предоставления услуг домашним пользователям в формате «тройной» услуги (triple-play): видео, голос и данные, и конкуренция на этом рынке только растет. Поэтому «Ниеншанц-Хоуму», имеющему абонентскую базу в 20 тысяч абонентов и предоставляющему различные услуги для жителей нескольких районов Петербурга, крайне важно предоставлять качественный и разнообразный набор услуг своим абонентам. «Ниеншанц-Хоум» давно двигался в данном направлении, повышая уровень технической компетенции своих специалистов, внедряя прогрессивные бизнес-процессы, нормативы на техническое обслуживание (например, время на восстановление узла сети в «Ниеншанц-Хоуме» составляет 4 часа) и естественно развивая собственную инфраструктуру.

Трафик генерируемый домашними пользователями имеет существенные особенности, отличающие его от трафика корпоративных клиентов. Например, в структуре трафика преобладает игровой трафик, трафик пиринговых приложений (Torrent, EMule, kazaa), которые при отстутствии ограничений способны выбрать всю доступную полосу пропускания и мешать работе приоритетных приложений. Также, весьма актуальна для домашних сетей задача защиты от вирусов и DDoS-атак. С этими двумя задачами неразрывно связана и третья: обеспечение возможности внедрения дополнительных сервисов для абонентов, что особенно актуально в условиях растущей конкуренции на рынке.

Несмотря на сложность и комплексность этих задач, их решение для компании «Ниешанц-Хоум» являлось приоритетным вопросом, напрямую связанным с позиционированием на рынке, развертыванию новых сервисов и повышению лояльности абонентов.

> ***"Обслуживание большой сети может развиваться либо по экстенсивному пути, когда увеличение работы и объемов компенсируется за счет привлечения большего количества сервис-инженеров, либо по интенсивному, когда идет усовершенствование оборудования на более интеллектуальное."***
>
> **— Дмитрий Новиков, Генеральный директор, «Ниеншанц-Хоум»**

Реализованное решение

Проведя сравнительный анализ возможных вариантов организации решения данных задач, технические специалисты компания «Ниеншанц-Хоум» остановились на оборудовании компании Cisco Systems – Service Control Engine 2020, являющегося частью концепции Cisco Systems по развертыванию инфраструктуры предоставления услуг – Service Exchange Framework (SEF).

Технологии, используемые в решении Cisco Service Control.

Решение Cisco SCE обладает возможностью контроля трафика приложений абонентов ШПД. Это позволяет создать различные пакеты услуг, определяющие полосу пропускания для трафика того или иного приложения. Например, ограничение полосы пропускания для P2P-трафика, задание квот на скачивание файлов, выделение стабильной полосы абоненту для Интернет-серфинга, блокировка трафика приложения, а так же перенаправление трафика на дополнительные серверы информационной безопасности для тщательной проверки. Данные политики, включая контроль спам-активности и блокировку DDoS-атак, действуют немедленно, что исключает дополнительные задержки, позволяющие спамеру или хакеру достигать своих целей.

Эта возможность значительно повышает уровень безопасности как для каждого отдельного абонента, так в целом сети оператора связи.

В компании «Ниеншанц-Хоум» было проведено тщательное тестирование решения Cisco SCE 2020 и после его успешных результатов, было принято решение о внедрении, а также была проведена интеграция с системой биллинга.

© Cisco Systems, Inc, 1992–2008 г.г. С сохранением всех прав. В этом документе содержится информация, свободно распространяемая Cisco.

Результаты внедрения

Генеральный директор «Ниеншанц-Хоум», Дмитрий Новиков:

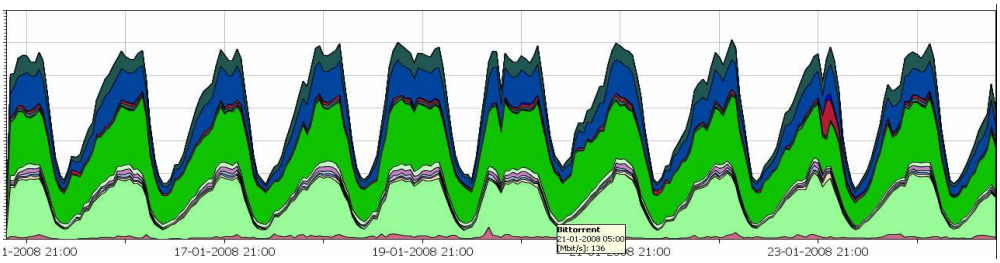
«Обслуживание большой сети может развиваться либо по экстенсивному пути, когда увеличение работы и объемов компенсируется за счет привлечения большего количества сервис-инженеров, либо по интенсивному, когда идет усовершенствование оборудования на более интеллектуальное.

Наша сеть выбрала второй вариант. В связи с большим темпом прироста абонентской базы за последнее время, мы установили новое оборудование Cisco SCE. И несмотря на недолгий срок эксплуатации, уже сейчас можно сделать выводы о существенном удобстве и экономии. Во-первых, сократился рост потребления внешнего Интернет трафика. Во-вторых, были оптимизированы расходы на персонал, т.е. возросшая абонентская база сети обслуживается фактически тем же количеством инженеров, как и год назад. Безусловно, увеличилось качество обслуживания, что особенно важно для «Ниеншанц-Хоум», поскольку гарантия стабильности и качества сети является одним из важнейших конкурентных преимуществ для нашей компании. Благодаря новому оборудованию гораздо быстрее подавляются вирусные атаки в сети и мы лучше знаем о реальном качестве предоставляемых услуг.»

Технический директор «Ниеншанц-Хоума», Кирилл Малеванов:

«Первым, наиболее заметным результатом внедрения Cisco SCE стало уменьшение загрузки маршрутизаторов, с которых была снята задача по ограничению скорости трафика абонентов. Данная задача была перенесена на Cisco SCE. Это позволило отложить необходимость модернизации маршрутизаторов. Сейчас, после нескольких месяцев эксплуатации, хочется отметить следующие факты:

– Мы стали понимать структуру трафика наших абонентов, научились дифференцировать его по протоколам, и предоставлять условия для разных видов трафика:

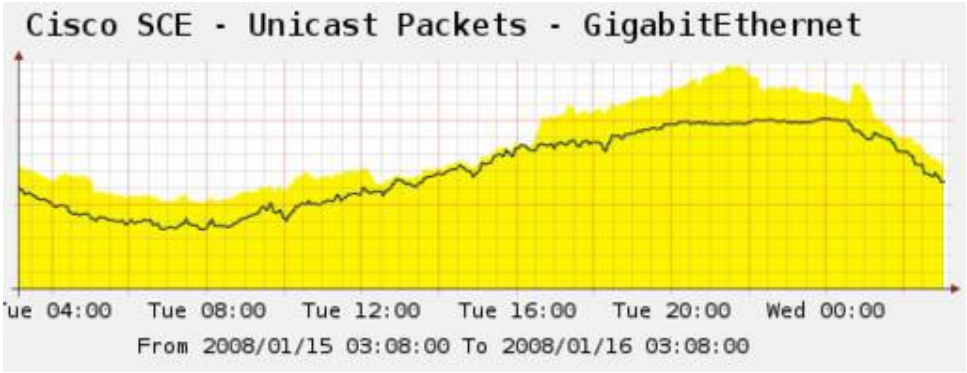


Структура трафика абонентов «Ниеншанц-Хоум».

© Cisco Systems, Inc, 1992–2008 г.г. С сохранением всех прав. В этом документе содержится информация, свободно распространяемая Cisco.

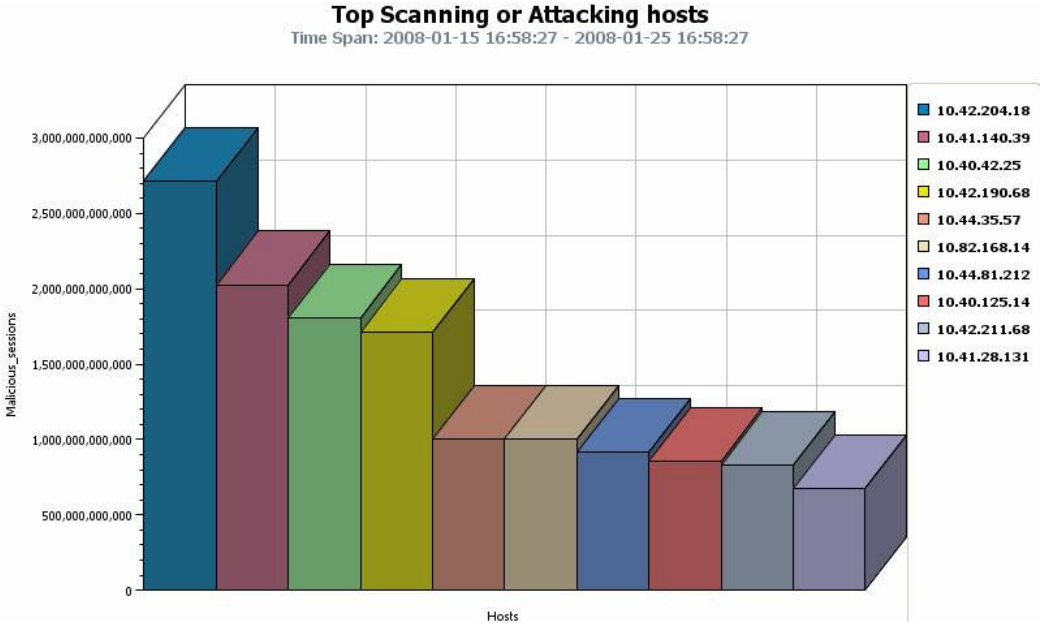
– Механизм обнаружения атак снизил загрузку на дежурных системных администраторов на 50%.

– Пользователям, которых решение Cisco SCE идентифицирует как зараженных вирусами, предлагается установка антивирусного программного обеспечения. В результате, в течение трех месяцев после внедрения, количество жалоб на спам и DDoS-атаки, исходящие из нашей сети, снизилось на порядок. Так, на графике ниже показан исходящий от абонентов трафик, поступающий на Cisco SCE. Превышение “желтого” графика над “синим” – это на 99% вирусный трафик. На выход же Cisco SCE не пропускает этот трафик, в итоге снижается загрузка на наши маршрутизаторы:



Идентификация вредоносного трафика в сети «Ниеншанц-Хоум».

– И мы можем определять, кто из пользователей больше всех генерирует вредоносного трафика:



Идентификация зараженных вирусами абонентов в сети «Ниеншанц-Хоум».

– Мощная система отчетов позволяет определять узкие места в нашей сети. При помощи решения Cisco SCE мы контролируем даже значения вариации задержки (jitter) на голосовом трафике и можем влиять на маршрутизацию трафика, исходя из этих данных.

© Cisco Systems, Inc, 1992–2008 г.г. С сохранением всех прав. В этом документе содержится информация, свободно распространяемая Cisco.

– Механизм оповещения пользователей и системных администраторов о наличии аномалий в трафике уменьшает время реакции персонала на появление вирусного трафика в сети.

Проанализировав при помощи Cisco SCE структуру трафика наших абонентов, мы приняли ряд действий по оптимизации внешних каналов и организации пиринга с другими сетями, и этот комплекс мер позволил снизить загрузку внешних каналов на 15-20 процентов.

На текущий момент мы готовимся к запуску дополнительных сервисов, возможность реализации которых предоставляет Cisco SCE.»

Системный инженер «Cisco Systems», Борис Хасанов:

«Cisco SCE – это уникальное решение, ориентированное для операторов широкополосного доступа. Оно позволяет решить целый комплекс взаимосвязанных задач:

- Получить подробную картину различных типов сетевого трафика, используемого абонентами.
- Оптимизировать нагрузку на сеть, за счет применения различных политик к трафику абонентов.
- Решить проблему с угрозами безопасности, исходящими от абонентов ШПД, такими как рассылки спама, DDoS-атаки и сканирование. Это помогает оператору минимизировать риск претензий третьих сторон, пострадавших от действий абонентов.

И, наконец, одно из главных достоинств Cisco SCE – это обеспечение возможности оператору по развертыванию дополнительных сервисов на сети и как следствие повысить лояльность своих абонентов, и увеличить свои доходы.»

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Для получения дополнительной информации о решении Cisco Service Control Engine, посетите нашу страницу в Интернет: http://www.cisco.com/go/servicecontrol/

О компании Cisco Systems

Cisco Systems, Inc. (NASDAQ: CSCO) – мировой лидер в области сетевых технологий, меняющих способы человеческого общения, связи и сотрудничества. Информация о решениях, технологиях и текущей деятельности компании публикуется на сайтах www.cisco.ru и www.cisco.com. Свежие новости Cisco можно найти в разделах http://www.cisco.com/global/RU/news/

© Cisco Systems, Inc, 1992–2008 г.г. С сохранением всех прав. В этом документе содержится информация, свободно распространяемая Cisco.

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 (327) 244-21-01
Факс: +7 (327) 258-46-60
www.cisco.ru
www.cisco.com

Cisco
Украина, 03038, Киев,
бизнес-центр
«Горизонт Парк»
(Horizon Park)
Ул. Николая Гринченко, 4В
Тел.: +38 (044) 391-36-00
Факс: +38 (044) 391-36-01
www.cisco.ua
www.cisco.com

Cisco
Азербайджан,
AZ 1065, Баку,
бизнес-центр «Карат»
Ул. М. Мухтарова, 201,
этаж 2
Тел.: +994 (50) 250-99-94
Факс: +994 (12) 437-48-20
www.cisco.ru
www.cisco.com

Cisco
Узбекистан, 100000,
Ташкент, бизнес-центр
«Инконель»
Ул. Пушкина, 75,
офис 605,
Тел.: +998 (71) 140-44-60
Факс: +998 (71) 140-44-65
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

Copyright © 2007 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or 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. (0406R)