

Cisco Expo 2011



PiN Telecom: ОПЫТ внедрения DPI на базе Cisco SCE

Кирилл Малеванов
malevanov@pntl.ru

innovate *together*

О компании

- Компания ПИН Телеком активно проводит политику слияния и поглощения на рынке ШПД Санкт-Петербурга
- 170 000 пользователей ШПД
- 3000 бизнес-клиентов

- Поглощены такие компании и бренды, как:
- Антхил
- GeneralNet
- Ниеншанц-Хоум
- Well-Com
- kspd.ru
- IntraStar



Первые шаги



Первые шаги

- Cisco SCE использовалась в сети Ниеншанц-Хоум. Это было первое внедрение SCE на сети оператора в России и СНГ
- Первоначальные задачи:
 - Нарезка полосы пропускания для пользователей
 - Оповещения об отрицательном балансе и блокировке
 - Спам-контроль и антиДОС



Первые шаги

- Простая интеграция с биллингом на базе CSV- файлов
- Широкий спектр настроек.
- Пакет – набор сервисов, возможно, с расписанием по часам и дням недели
- Сервис – набор протоколов применительно к зонам
- Протокол – вид сессии. HTTP Browsing, BitTorrent, Skype
- Зона – список IP-адресов



Подсчет трафика



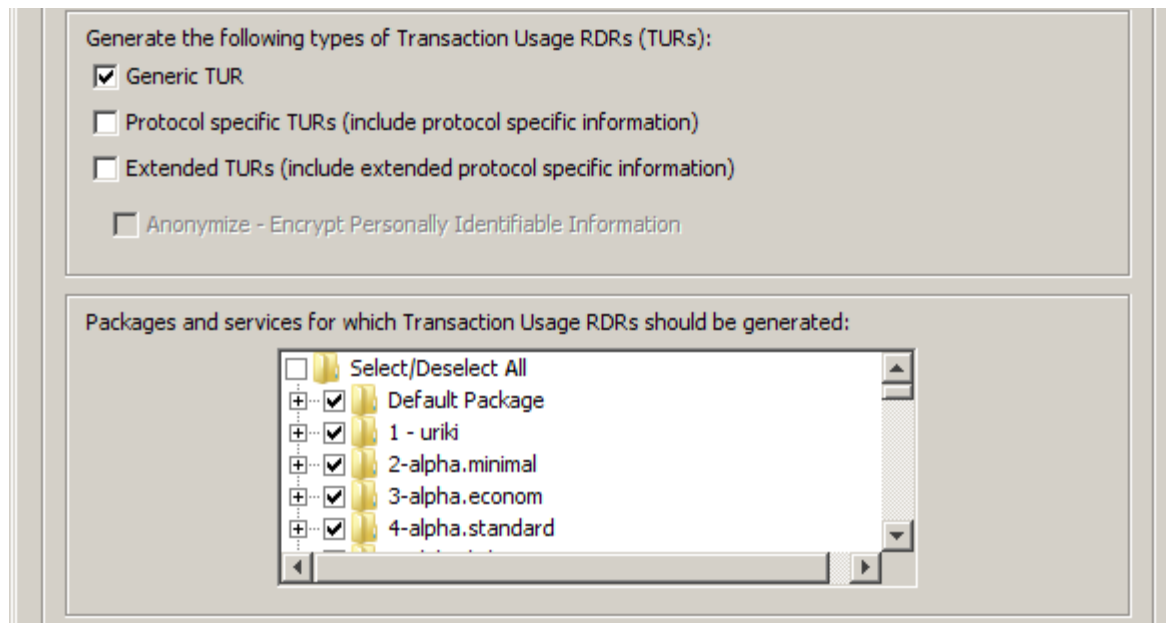
Подсчет трафика

- RDR – Raw Data Records
- Собственная утилита-коллектор.

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	See Universal RDR Fields .
PACKAGE_ID	UINT16	See Universal RDR Fields .
SERVICE_ID	INT32	See Universal RDR Fields .
PROTOCOL_ID	INT16	See Universal RDR Fields .
SKIPPED_SESSIONS	INT32	Number of unreported sessions since the previous RDR.
SERVER_IP	UINT32	See Universal RDR Fields .
SERVER_PORT	UINT16	See Universal RDR Fields .
ACCESS_STRING	STRING	See Universal RDR Fields .
INFO_STRING	STRING	See Universal RDR Fields .

Подсчет трафика

- Подсчет трафика, исходя из subscriber name
- Subscriber Usage Record – почти Radius Accounting
 - Задание сервисов в RDR
 - Задание сервисов, на которых отливка RDR не происходит



Подсчет трафика

- Transaction Usage Record – почти Netflow v5

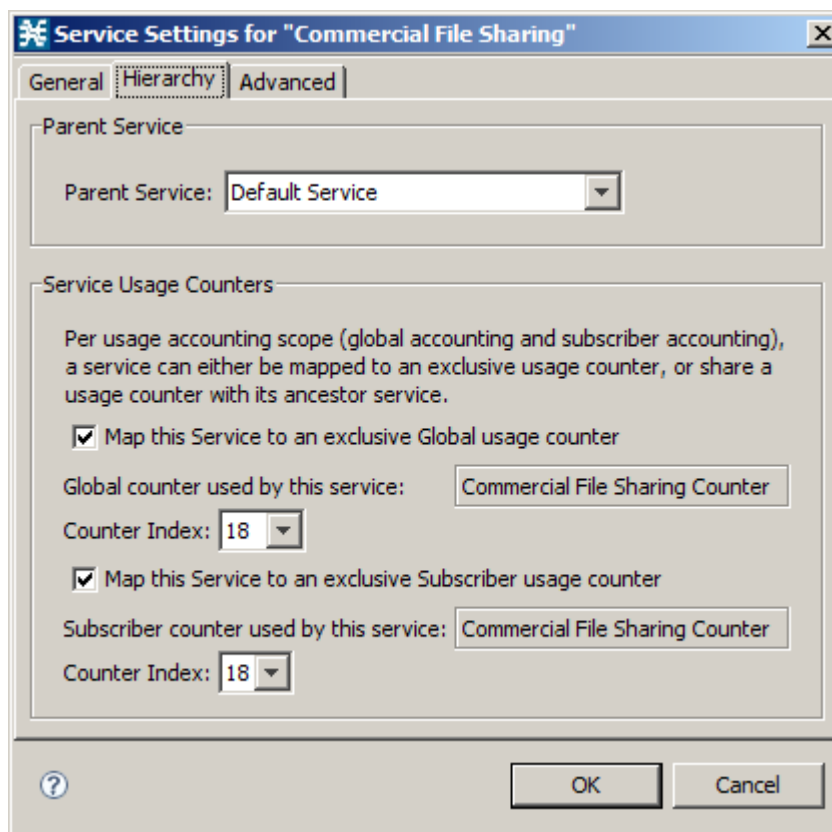
RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	See Universal RDR Fields .
PACKAGE_ID	UINT16	See Universal RDR Fields .
SERVICE_ID	INT32	See Universal RDR Fields .
PROTOCOL_ID	INT16	See Universal RDR Fields .
SKIPPED_SESSIONS	INT32	Number of unreported sessions since the previous RDR.
SERVER_IP	UINT32	See Universal RDR Fields .
SERVER_PORT	UINT16	See Universal RDR Fields .
ACCESS_STRING	STRING	See Universal RDR Fields .
INFO_STRING	STRING	See Universal RDR Fields .

- Максимальный поток TUR – 20К записей в секунду.



Подсчет трафика

- Разделение по сервисам



Спам-контроль и DOS-контроль



Спам-контроль

- Спам-контроль на основании данных о количестве SMTP-сессий
- Разные действия для разных тарифных пакетов – от оповещения NOC до блокировки действий пользователя.

Configure spam detection threshold and mitigation action per package:

Package	Detection threshold	Send RDR	Block selected service traffic	Notify subscriber (HTTP)	Mirror SMTP traffic
1100 - unlim.light.3.0 - 10/5	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1110 - unlim.light.4.0 - 100/6	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1111 - unlim.light.4.0 +podar...	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1200 - unlim.optimal.3.0 - 20/10	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1210 - unlim.optimal.4.0	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1211 - unlim.optimal.4.0 + po...	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1250 - test parental control	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1310 - unlim.prof.4.0	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1311 - unlim.prof.4.0 + poda...	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1410 - unlim.premium.4.0	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1510 - unlim.delux	25 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
1511 - shkol`niy	10 session per 30 seconds	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMTP virus	None
2000 - rabochy polden	10 session per 30 seconds	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	None
2001 - rabochy polden+voip	10 session per 30 seconds	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	None

DOS-контроль

- DOS-контроль на основании данных о количестве новых сессий на различные ресурсы

Anomaly Detector Wizard

Anomaly Detection Thresholds
Define attack detection thresholds, or use the Default Detector's values

Malicious Traffic Detection Thresholds

Use the Default Detector's settings

An anomaly will be detected once flow rate exceeds this threshold.

Flow Open Rate (flows/sec)

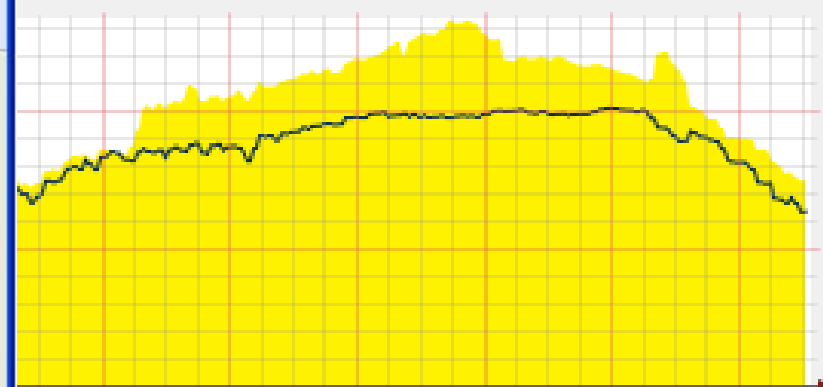
An anomaly will be detected once suspected flow rate exceeds threshold AND suspected flows ratio exceeds threshold.

Suspected Flows Rate (flows/sec)

Ratio of Suspected Flow Rate (%)

< Back Next > Finish Cancel

Ports - GigabitEthernet



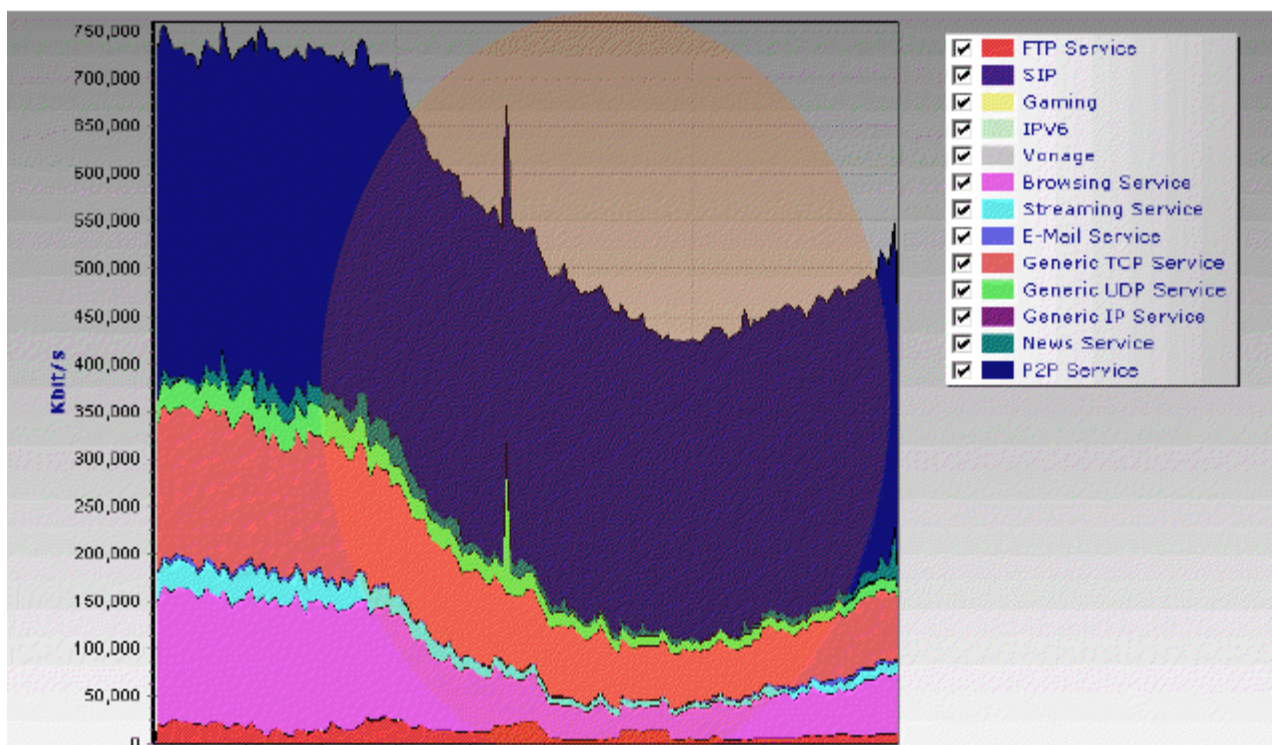
Tue 16:00 Tue 20:00 Wed 00:00
To 2008/01/16 03:08:00

Борьба с P2P



Борьба с P2P

- Противостояние брони и снаряда
- Новые протокол-паки каждые 3 месяца



Борьба с P2P

- 4 класса трафика внутри сети
- Классификация P2P как трафика с наименьшим приоритетом
- Лимитирование количества сессий для разных пакетов

The screenshot displays the Service Configuration Editor interface. On the left, a tree view shows various policies, with '1210 - unlim.optimal.4.0' selected. The main pane shows a table of rules for this policy:

Rule	Status
Default Rule	controlled
T1	controlled
T2	controlled
ICMP	controlled
Local traffic	controlled
yandex	controlled
P2P	controlled
T1	controlled
T2	controlled
Bittorent uTP	blocked




The right pane shows the 'Edit Rule for Service "P2P"' configuration. The 'Control' tab is active, and the 'Limit concurrent flows of this Service' checkbox is checked, with the value set to 100. The 'CoS' dropdown is set to 'BE'.

Борьба с P2P

- Лимитирование общей полосы пропускания для подписчиков

Global Upstream Policy

Total Link Limit: Link 1: 10000.0 Mbps; Link 2: 10000.0 Mbps; Link 3: Unlimited ...

Upstream	Policy Description
 P2P high priority	Link 0 Bandwidth Limit: 6000.0 Mbps, 8000.0 Mbps ; Link 1 ...
 P2P low priority	Link 0 Bandwidth Limit: 4000.0 Mbps ; Link 1 Bandwidth Limit: ...
 Default Global Controller	Link 0 Bandwidth Limit: 10000.0 Mbps ; Link 1 Bandwidth Limit: ...

Родительский контроль

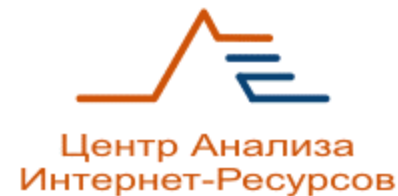


Родительский контроль

- 91% родителей говорят, что **Интернет помогает их детям** знакомиться с интересующими их материалами
- 76% родителей говорят, что они хотели бы **сделать Интернет более безопасным** для детей
- 88% родителей предпочитают контролировать действия ребенка в Интернете, а не соблюдать конфиденциальность жизни ребенка
- 87% родителей проверяют информацию о действиях ребенка в Интернете несколько раз в месяц
- Данные предоставлены Common Sense Media (июнь 2006 г.)
(<http://www.commonsensemedia.org/news/press-releases.php?id=23>)

Родительский контроль

- Решение совместно с ЦАИР
- Классификация сайтов по категориям



Enable HTTP content filtering

Package Settings Database Settings

This section displays the information contained in the imported Database Settings XML file

Vendor Name: CAIR

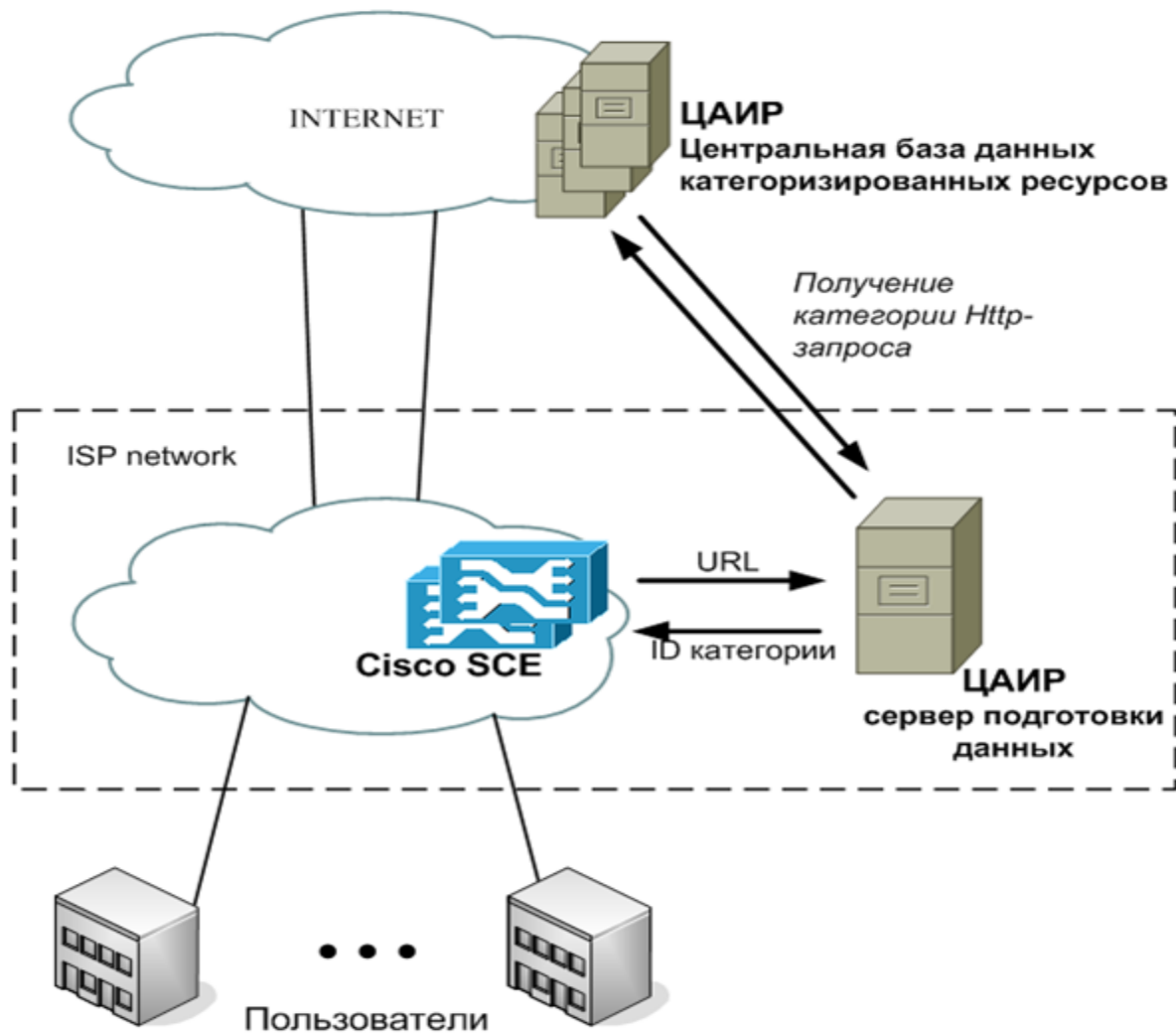
Vendor Information: CAIR URL Content Database
Content Filtering Settings for SCA BB 3.0.3

Categorize Content by: WholeUrl

Content Categories:

- alcohol
- porno
- advertising, banner servers
- authority
- auto
- cinema
- construction and renovation
- consumer
- cookery
- countrv house

Родительский контроль



Родительский контроль

- Настройка пакетов на Cisco SCE

801 - super.light + podaroc (up 3, dc	P2P	controlled ; unlimited quota
900 - super.optimal	T1	controlled ; unlimited quota
901 - super.optimal + podaroc (up 5,	T2	controlled ; unlimited quota
1000 - super.maximum	HTTP Browsing with Categories	controlled ; unlimited quota
1001 - super.maximum + podaroc (up	HTTP Browsing.parental	redirected
1100 - unlim.light.3.0 - 10/5		
1110 - unlim.light.4.0 - 100/6		
1111 - unlim.light.4.0 +podarok - 100		
1200 - unlim.optimal.3.0 - 20/10		
1210 - unlim.optimal.4.0		
1211 - unlim.optimal.4.0 + podarok (
1250 - test parental control		

Set CoS for flows of this Service to

Redirect profile for this service:

Redirect destination URLs

HTTP Browsing:

HTTP Streaming:

Родительский контроль

- Итоги внедрения
 - За 2 месяца тестирования – 600 подписчиков (из 120К)
- Регулярность использования
 - 30-50 человек в день производят манипуляции с включением-выключением



Работа с бизнес-клиентами



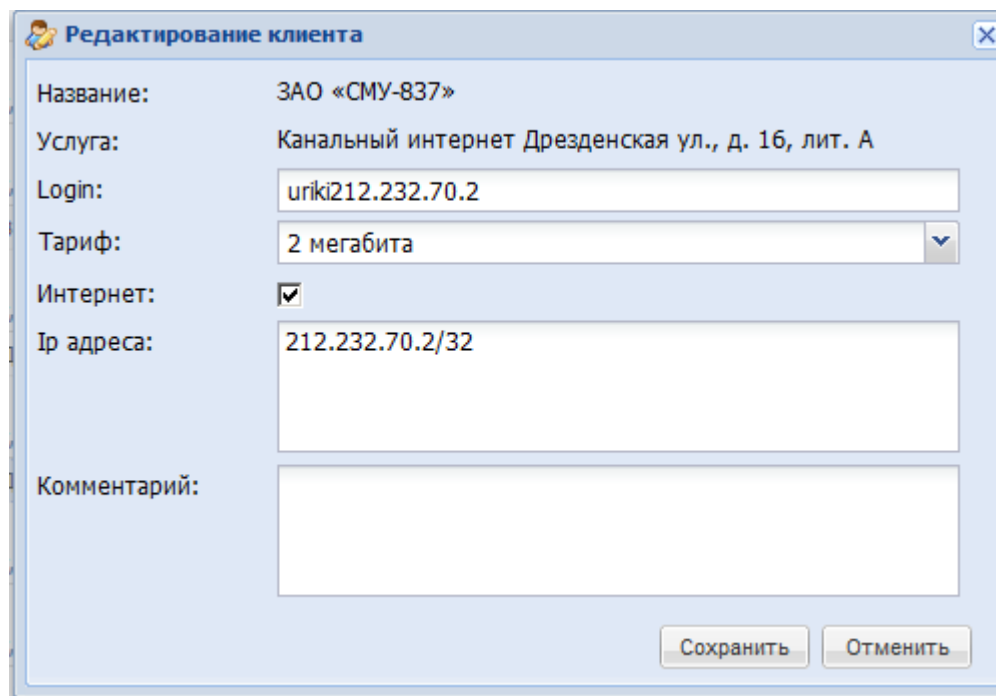
Работа с бизнес-клиентами

- Идея: включение-выключение услуг должно происходить без участия «технарей»

Список клиентов						
+	Название	Адрес	Login	Тариф	Ip	Интернет
Договор	Услуга	Login	Тариф	Ip адреса	Интер...	
+	ЗАО «НОРДВЕГ» Адрес: 198035, г. Санкт-Петербург, Двинская ул., д. 16, корп. 2					
+	ЗАО «НПФ «Октант» Адрес: 196128, г. Санкт-Петербург, Варшавская ул., д. 19, корп. 2					
D-336-11	Канальный интернет Варшавская ул...	uriki212.232.69.58	1 мегабит		212.232.69.58/32	on
+	ЗАО «Первая Трубная Компания» Адрес: 198035, г. Санкт-Петербург, Двинская ул., д. 10, корп. 2					
D-337-11	Канальный интернет Двинская ул., д...	uriki212.232.68.102	5 мегабит		212.232.68.102/32	on
+	ЗАО «СМУ-837» Адрес: 194017, г. Санкт-Петербург, Дрезденская ул., д. 16, лит. А					
D-315-11	Канальный интернет Дрезденская у...	uriki212.232.70.2	2 мегабита		212.232.70.2/32	on

Работа с бизнес-клиентами

- Использование Cisco SCE Java API для изменения информации о клиенте



The image shows a dialog box titled "Редактирование клиента" (Edit Client). It contains the following fields and controls:

- Название:** ЗАО «СМУ-837»
- Услуга:** Канальный интернет Дрезденская ул., д. 16, лит. А
- Login:** uriki212.232.70.2
- Тариф:** 2 мегабита (dropdown menu)
- Интернет:**
- Ip адреса:** 212.232.70.2/32
- Комментарий:** (empty text area)

At the bottom right, there are two buttons: "Сохранить" (Save) and "Отменить" (Cancel).

Итого



Итого

- Использование Cisco SCE для задач ISG
 - Гибкие тарифные планы
 - Приоритезация трафика по приложениям
 - Уведомления клиентов об изменениях в обслуживании
 - Новые услуги – родительский контроль
- Отчетность по трафику для биллинга
 - Совместимость с текущими и будущими биллинг-системами
- Работа совместно с BSS для бизнес-клиентов
 - Снижение нагрузки на техподдержку
- SPAM и DOS-контроль сети
- Масштабируемость решения



Cisco Expo 2011



Спасибо!

Просим Вас заполнить анкеты.
Ваше мнение очень важно для нас.

innovate *together*