Що ж до експлуатації – слід брати до уваги грози, коли можуть виходити з ладу цілі сегменти мережі, і навряд чи у периферійних місцевостях, де надають послуги безпроводового інтернету, зможуть самостійно лагодити обладнання WiMAX.

Для швидкого розгортання та зручності налаштування мережі WMAN низької собівартості розглянуті рішення мають право на гідне місце у сучасних потребах операторів.

Література

1. KarlNet's TurboCell™: Enhancing the Capabilities of Standard 802.11.
2. Стандарт IEEE 802.11n™. – 2009.

УДК 004.725.5

Дугин А. О., асп. *(Украинский НИИ связи).*

ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ ПРИ ВНЕДРЕНИИ СИСТЕМ АНАЛИЗАТРАФИКА В КОРПОРАТИВНОЙ СЕТИ

Дугін А. О. Проектування архітектури при впровадженні систем аналізу трафіка в корпоративній мережі. Запропоновано архітектурно-топологічні вимоги до точок встановлення сенсорів мережевого аналізу в корпоративній мережі. Вимоги ґрунтуються на практичних особливостях використання універсальних мережевих технологій і протоколів в корпоративній інфраструктурі.

Ключові слова: МЕРЕЖЕВИЙ АНАЛІЗ, АНАЛІЗ ТРАФІКА МЕРЕЖЕВІ СЕНСОРИ

Дугин А. О. Проектирование архитектуры при внедрении систем анализа трафика в корпоративной сети. Предложены архитектурно-топологические требования к точкам установки сенсоров сетевого анализа в корпоративной сети. Требования основаны на практических особенностях использования универсальных сетевых технологий и протоколов в корпоративной инфраструктуре.

Ключевые слова: СЕТЕВОЙ АНАЛИЗ,АНАЛИЗ ТРАФИКА, СЕТЕВЫЕ СЕНСОРЫ

Dugin A. O. Architecture planning with traffic analysis systems implementation in the corporate network. The architectural and topological requirements are proposed for the points of traffic analysis sensors implementation in the corporate network. These requirements are based on the practical aspects of the universal network technologies usage in the corporate infrastructure.

Keywords: NETWORK ANALYSIS, TRAFFIC ANALYSIS, NETWORK SENSORS

Сеть передачи данных крупных предприятий логически делится на 3 уровня. Уровень, на котором к коммутаторам подключаются пользователи и конечные узлы, чаще всего называют уровнем доступа. Маршрутизация между подсетями уровня доступа, резервирование шлюза по умолчанию, применение межсетевого экранирования и балансировки трафика конечных узлов производится на уровне агрегации. Высокоскоростная коммутация и маршрутизация, резервирование и эффективное использование каналов осуществляется на уровне ядра сети [1]. Уровни доступа и агрегации можно выделить как для пользовательского сегмента, где конечными узлами будут пользовательские ПК, так и для сегментов центров обработки данных (ЦОД), в котором конечными узлами могут быть виртуальные либо физические сервера.

Перед внедрением систем сетевого анализа нужно определить необходимость их установки в пользовательском сегменте. Необходим тщательный анализ того, какой трафик будут генерировать пользовательские станции, и какой интерес он представляет. Типы трафика в корпоративных сетях можно определить следующие:

– технологический: управление ПК и учетными записями с централизованного сервера, обновление ОС, приложений, антивирусных баз;

– служебный: электронная почта, сетевые бизнес-приложения, прочие клиент-серверные взаимодействия в пределах локальной сети;

– личный: сообщения электронной почты, служб обмена мгновенными сообщениями, трафик других приложений, информация, полученная/передання через веб-браузер.

Анализ трафика пользовательских станций может представлять интерес для подразделений компании, ответственных за: *администрирование* рабочих мест пользователей; *поддержку* сетевой инфраструктуры; *оптимизацию* сетевой архитектуры; *контроль* соблюдения политик информационной безопасности.

Если для подразделений поддержки и оптимизации инфраструктуры будет представлять интерес в основном информация об установленных сессиях и переданном/полученном объеме трафика, то подразделениям информационной безопасности потребуется анализ всех уровней модели OSI. Подразделениям, ответственным за администрирование рабочих станций, наибольшую пользу будет представлять информация о приложениях, генерирующих те или иные пакеты.

В серверных сегментах, которые также называются центрами обработки данных (ЦОД), в зависимости от профиля деятельности компании реализуются такие функции как обработка, хранение, распространение и защита информации, предоставление услуг и т. п. Даже у предприятий, не специализирующихся на информационных технологиях и телекоммуникациях, но имеющих большие объемы данных и определенный набор серверов, обеспечивающих основные функции, трудно переоценить роль ЦОД в бизнесе. Соответственно, в первую очередь системы анализа трафика устанавливаются в серверных сегментах инфраструктуры.

Предположим, данный фрагмент корпоративной сети имеет архитектуру, изображенную на рис. 1. Для внедрения систем сетевого анализа необходима либо установка ответвителей трафика на соответствующих интерфейсах взаимосвязи сетевых устройств, снимающих копию трафика с линии и подающих на сенсоры, либо конфигурация «зеркалирования» трафика на коммутаторах и маршрутизаторах.

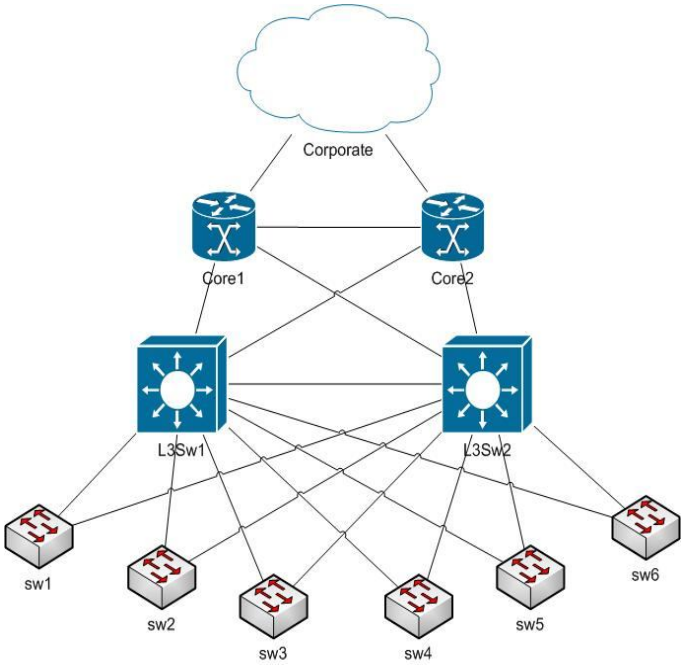

Рис. 1. Фрагмент корпоративной сети

При использовании технологий «зеркалирования» трафика, таких как SPAN (Switch Port Analyzer) [1, 2] либо VACL (VLAN Access Control List) Capture [3] полная копия пакетов с определенных физических либо логических интерфейсов направляется на выделенные порты, к которым подключаются сетевые сенсоры IDS/IPS. «Зеркалировать» трафик, также называемый SPAN – либо VACL-capture сессией, можно на каждом коммутаторе уровня доступа sw1...sw6 и дополнительно L3Sw1 и L3Sw2. Но, таким образом, возрастет нагрузка на сетевой сенсор, что скажется на определении требований к его количеству интерфейсов, производительности и стоимости. Кроме того, отрицательной стороной данного решения будет большое количество продублированных пакетов, приходящих на IDS. Более оптимальным решением с точки зрения дизайна сети будет подключить сенсор к коммутаторам со следующими топологическими характеристиками (рис.2): *spanning*-treeroot, secondary root [4]; *включен* непосредственно в L3-устройство (router, firewall) либо осущест-вляющий терминацию подсетей; *топологически* расположен ближе всего к HSRP/VRRPmaster либо активной ноде группы отказоустойчивости кластера межсетевых экранов [5].

Данным требованиям соответствуют коммутаторы L3Sw1 и L3Sw2.

Независимо от тонкостей дизайна сети, необходимо анализировать трафик с обоих вышеупомянутых коммутаторов. Копия трафика с определенных физических или логических интерфейсов направляется на сетевой сенсор.

В зависимости от модели и производительности, устанавливается либо один сенсор на оба коммутатора, либо по одному на коммутатор (см. рис. 2).

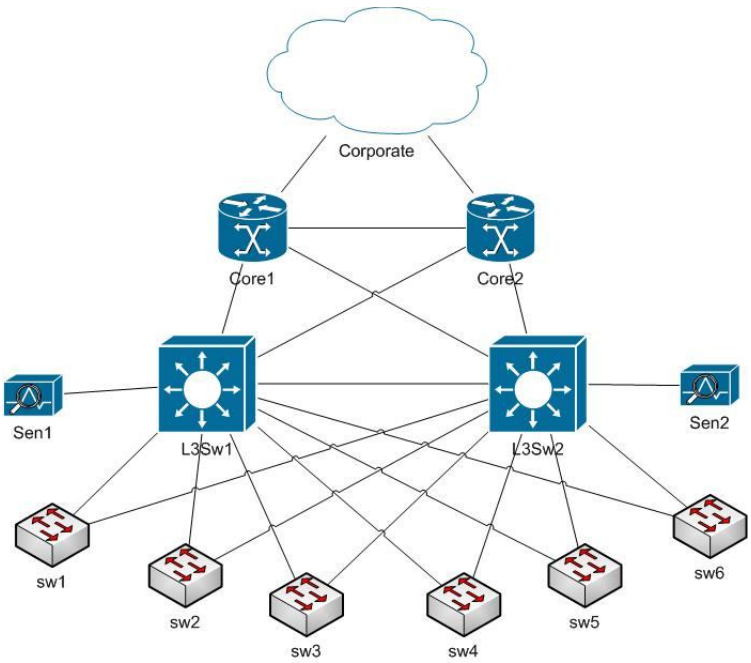

Рис. 2. Фрагмент корпоративной сети с сетевыми сенсорами

Сенсоры Sen1 и Sen2 могут быть как одиночные сенсоры, так и разными «слушающими» интерфейсами одного сенсора, так и элементами кластера сетевых сенсоров.

После выбора коммутатора необходимо определить, какой трафик требуется анализировать – генерируемый узлами данного сегмента до перехода в ядро сети (участок sw1-6 <->L3Sw1-2), в том числе внутрисегментный и поступивший из корпоративной сети в данный сегмент, либо входящий трафик из других сегментов и исходящий из данного в другие сегменты (участок Core1,2 <->L3Sw1,2).

В случае установки ответвителей трафика «в разрыв» возможными вариантами размещения сенсоров на схеме (рис. 1) будут участки перехода между уровнями агрегации и ядра (рис.3) и между коммутаторами уровня доступа и агрегации (рис. 4).

На участке L3Sw*x*-Corex (рис. 3) ответвитель размещается в том случае, когда стоит задача инспектировать трафик, инициируемый данным сегментом в сторону остальных участков сети, а также входящий из других сегментов трафик до фильтрации. Существенным недостатком подключения сенсора на данном участке является отсутствие контроля информационных потоков внутри сегмента.

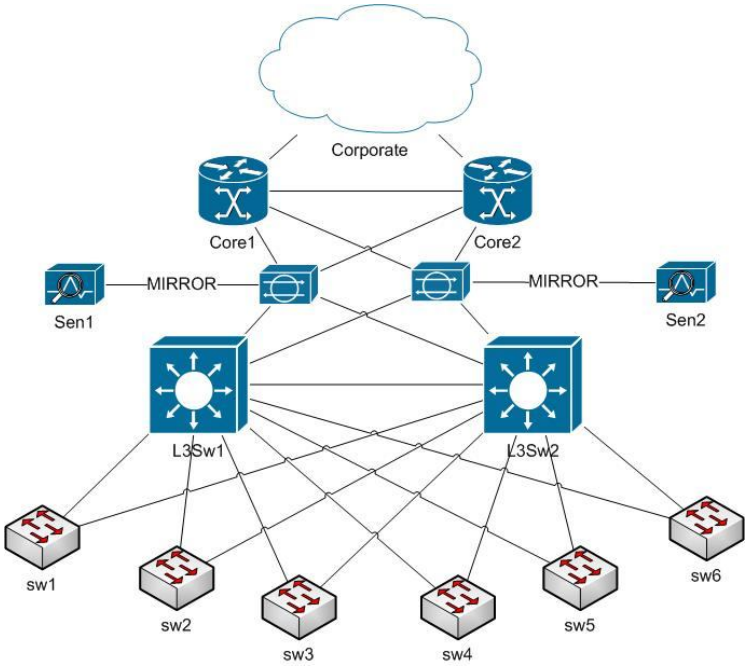

Рис. 3. Ответвители «в разрыв» на участке агрегация-ядро

Копирование трафика с линийна участках sw*1-6* – L3Sw*1-2* (рис. 4) позволяет осуществлять как анализ трафика, предназначенного для других сегментов сети, так и внутрисегментные взаимодействия.

Однако в данном случае анализаторы будут обрабатывать большое количество продублированных пакетов и широковещательный трафик внутри подсетей инфраструктурного сегмента, что может быть как плюсом, так и минусом в зависимости от поставленных целей.

Выводы. Правильное определение топологического места установки сенсоров систем сетевого анализа позволяет снизить затраты, минимизировать анализ дублирующегося либо ненужного трафика.

Наиболее рационально анализировать трафик коммутаторов уровня агрегации, а при установке ответвителей «в разрыв» возможны варианты на участках агрегация-доступ и агрегация-ядро в зависимости от поставленных задач.

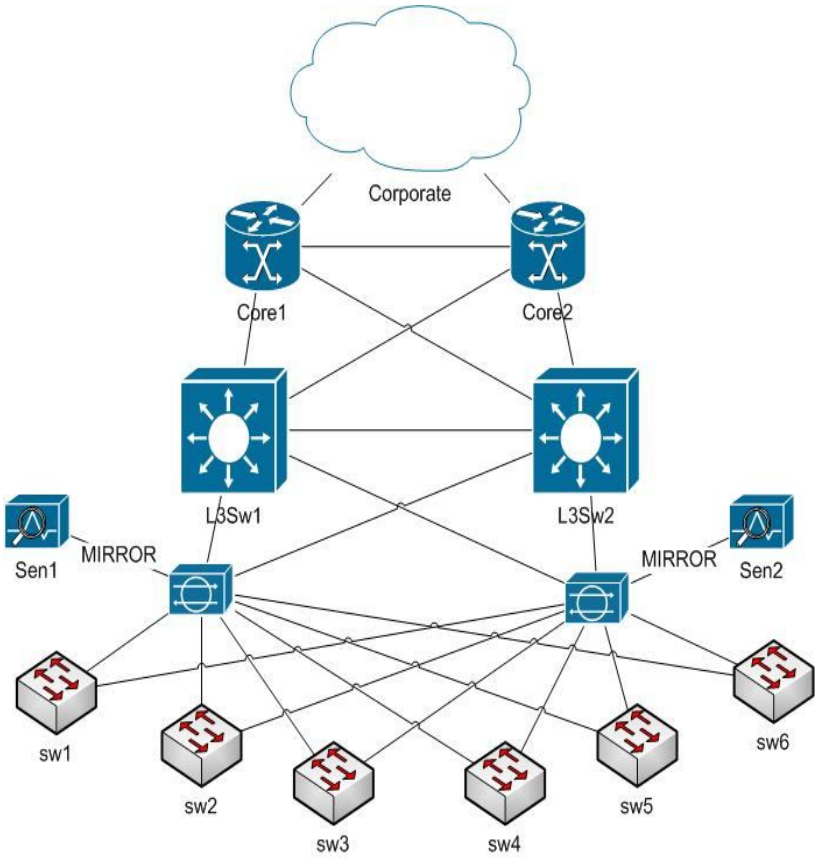

Рис. 4. Ответвители «в разрыв» на участке доступ-агрегация

Литература

1. Enterprise Campus 3.0 Architecture: Overview and Framework. Hierarchy [Електронний ресурс] // – Режим доступу: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp708780 (20.08.2012).

2. Catalyst Switched Port Analyzer (SPAN) Configuration Example [Електронний ресурс] // – Режим доступу: http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml

3. VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running Cisco IOS Software [Електронний ресурс] // – Режим доступу: http://www.cisco.com/en/US/tech/tk389/tk814/technologies_configuration_example09186a00808122ac.shtml

4. Cisco Data Center Infrastructure 2.5 Design Guide - Spanning Tree Scalability [Електронний ресурс] // – Режим доступу: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_5.html

5. Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks [Електронний ресурс] // – Режим доступу: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094afd.shtml