АНАЛИЗ ТРАФИКА УЧРЕЖДЕНИЯ КАК СПОСОБ ОПРЕДЕЛЕНИЯ УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

Г.М. Михайлов, Ю.П. Рогов, А.М. Чернецов

Вычислительный центр им. А.А. Дородницына РАН

Одним из способов определения уязвимости информационной безопасности корпоративной сети является анализ входящего и исходящего Internet-трафика. Для решения этой проблемы одним из способов является применение специализированного ПО ManageEngine (ZOHO COPR) Netflow Analyzer [1].

ВЦ РАН впервые проводил подобный анализ в ноябре 2009 г. силами сторонней организации [2]. Целью этого анализа являлась апробация текущей конфигурации локальной вычислительной сети (ЛВС) и внешнего канала ВЦ РАН, выявление слабых мест в конфигурации и выдача рекомендаций по модернизации с учетом выявленных замечаний.

Нужно отметить, что доступ пользователей и серверных приложений из ЛВС ВЦ РАН в Интернет осуществляется через канал, организованный между маршрутизатором Cisco2851 и маршрутизаторами Интернет-провайдера. В случае выхода из строя основного нашего маршрутизатора в работу включается запасной (Cisco 2821) [3,4]. Единовременно в работе находится только одно из установленных соединений – в соответствии с результатом работы протокола BGP (Border Gateway Protocol, протокол граничного шлюза). Такой режим работы обусловлен договоренностью с провайдером для совместного мониторинга канала связи и возможностью переключения на резервный маршрутизатор провайдера [4].

Тестирование производительности Интернет-канала проводилось с использованием инструментов IP SLA UDP Jitter с использованием программного обеспечения PRTG Monitor [5].

По итогам данного анализа было принято решение о закупке ПО на постоянной основе с возможностью проводить исследования и анализ полученных данных самостоятельно.

Анализ трафика позволяет узнать такие параметры, как процент загруженности канала связи, выделить узлы ЛВС, наиболее активно принимающие/передающие трафик как вне ЛВС, так и внутри ее. Общий объем трафика за месяц (2014-04-25 – 2014-05-25) составил: входящего 378.46 ГБ, исходящего — 574.5 ГБ.

На рис.1 представлена диаграмма (за период 1 месяц) использования трафика по протоколам. На рис.2 представлена диаграмма по трафику с внешними IP-адресами.

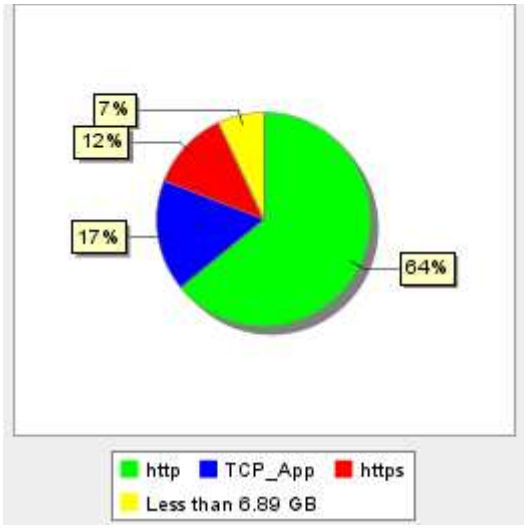

Рис. 1

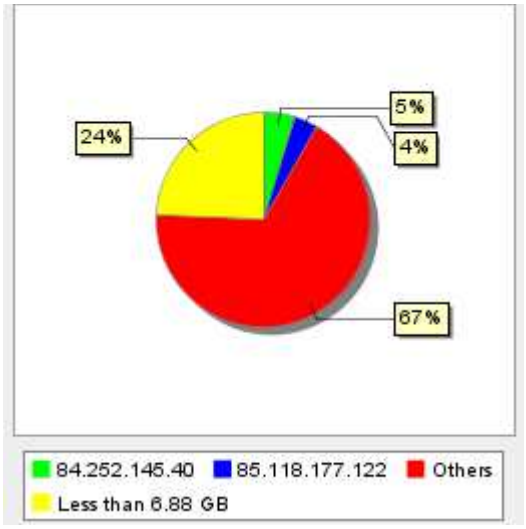

Рис. 2

К примеру, объем почтового (SMTP - Simple Mail Transfer Protocol) трафика за 1 месяц составил всего лишь 5.19 ГБ, что составило менее 2%. К удивлению авторов, на *почетном* 11 месте оказался протокол ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений), который на 95% своего объема был занят трафиком между pop3.ccas.ru (ВЦ РАН) и client.yota.ru.

Как видно из рис.1, 17% трафика занимает «TCP_App». Это означает, что программа не смогла распознать конкретный используемый протокол. Поэтому требуется «ручная» работа. Открывая протокол, мы получаем диаграмму, представленную на рис.3. Теперь можно анализировать трафик уже каждого конкретного IP-адреса из ЛВС ВЦ РАН и выяснить, что, куда и зачем передается. Не менее интересным является проведение

анализа трафика внутри ЛВС. В качестве примера приведем на рис.4 IPV6 трафик между двумя узлами ЛВС. Отметим, что общий объем IPV6-трафика в vlan составляет 100 ГБ.

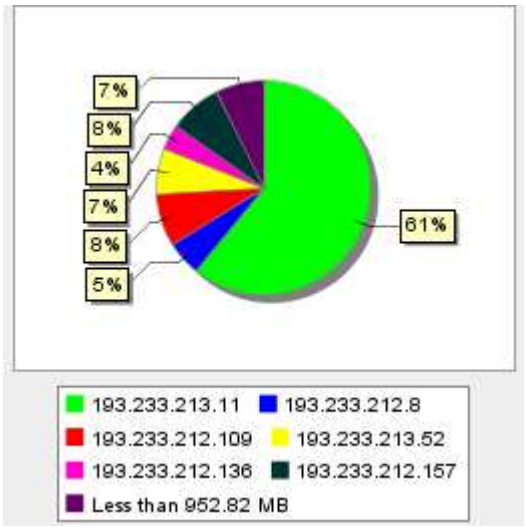

Рис. 3.

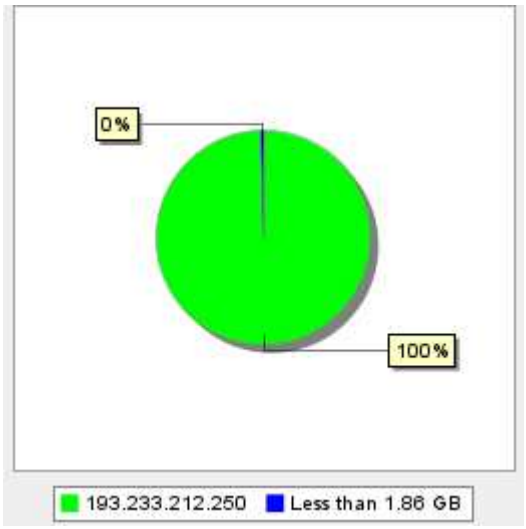

Рис. 4.

Очевидно, что на данную повышенную активность необходимо обратить пристальное внимание. В данном конкретном случае все в порядке, однако, возможны и другие виды «активности» (вирусы, не целевое использование трафика, и т.д.).

Приведенные методы анализа являются предварительными, но даже их применение может позволить очертить круг проблем, в том числе указанных выше. В этом случае понадобятся как аппаратно-программные средства, так и административные действия со стороны руководства и системных администраторов корпоративной сети для жесткого регулирования работы этой сети. Другими словами, придется принимать явно не популярные среди пользователей сети меры по внедрению корпоративной политики или правил работы в локальной сети.

ЛИТЕРАТУРА:

1. URL: http://www.manageengine.com (дата обращения 16.05.2014)
2. Ю.П Рогов, А.М Чернецов "Аппаратно-программные средства и развитие инфраструктуры ИВС ВЦ РАН" // М.: Изд-во ВЦ РАН, 2010, 120 с.
3. Г.М Михайлов, Ю.П Рогов, А.М Чернецов "Инфраструктура локальной компьютерной сети академического учреждения и вопросы обеспечения безопасности и защиты информации" //Материалы Всероссийской научной конференции "Научный сервис в сети ИНТЕРНЕТ", Новороссийск, 20-25 сентября 2010 г., Изд-во Московского Университета, с. 98-101
4. Г.М. Михайлов, Ю.П.Рогов, А.М.Чернецов "О некоторых особенностях построения ИВС ВЦ РАН" //М.: Изд-во ВЦ РАН, 2011, 41 с.
5. URL: http://www.paessler.com (дата обращения 19.05.2014)