Сетевое управление и мониторинг

Обзор NetFlow

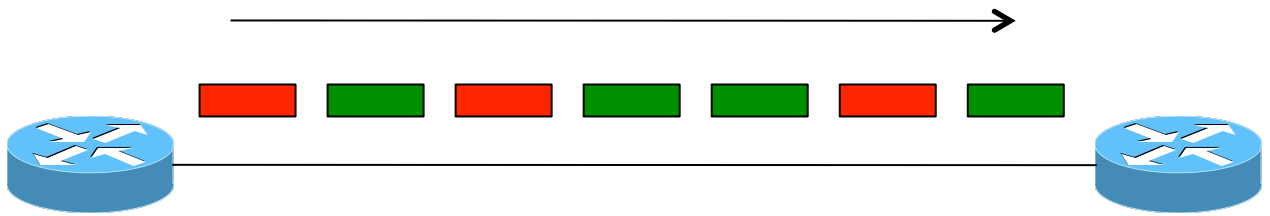
Содержание

1. **Netflow**
   - Что это такое и как оно работает
   - Использование и приложения
2. **Создание и экспорт записей потоков**
3. **Nfdump и Nfsen**
   - Архитектура
   - Использование
4. **Лабораторная работа**

Что такое поток NetFlow?

- Набор взаимосвязанных пакетов
- Пакеты, относящиеся к одному транспортному соединению, например
  - TCP, одинаковые IP отправителя (src IP), src порт, IP получателя (dst IP), dst порт
  - UDP, одинаковые src IP, src port, dst IP, dst port
  - Некоторые инструменты считают “двунаправленные потоки” (т.е. A->B и B->A) частью одного потока

Простые потоки



= Пакет, приналежащий потоку X

= Пакет, приналежащий потоку Y

Определение потока в Cisco IOS

Однонаправленная последовательность пакетов, разделяющих:

1. IP адрес отправителя
2. IP адрес получателя
3. Порт отправителя для UDP или TCP, 0 для других протоколов
4. Порт получателя для UDP или TCP, тип и код для ICMP, 0 для других протоколов
5. Протокол
6. Входящий интерфейс (SNMP ifIndex)
7. Тип сервиса IP

IOS: какие из этих шести пакетов в одних и тех же потоках?

	Src IP	*Dst IP*	*Protocol*	*Src Port*	*Dst Port*
A	1.2.3.4	5.6.7.8	6 (TCP)	4001	22
B	5.6.7.8	1.2.3.4	6 (TCP)	22	4001
C	1.2.3.4	5.6.7.8	6 (TCP)	4002	80
D	1.2.3.4	5.6.7.8	6 (TCP)	4001	80
E	1.2.3.4	8.8.8.8	17 (UDP)	65432	53
F	8.8.8.8	1.2.3.4	17 (UDP)	53	65432

IOS: какие из этих шести пакетов в одних и тех же потоках?

	Src IP	*Dst IP*	*Protocol*	*Src Port*	*Dst Port*
A	1.2.3.4	5.6.7.8	4 (TCP)	4001	22
B	5.6.7.8	1.2.3.4	4 (TCP)	22	4001
C	1.2.3.4	5.6.7.8	6 (TCP)	4002	80
D	1.2.3.4	5.6.7.8	6 (TCP)	4001	80
E	1.2.3.4	8.8.8.8	17 (UDP)	65432	53
F	8.8.8.8	1.2.3.4	17 (UDP)	53	65432

Как насчет “C” и “D”?

Учет потоков

Сводка всех пакетов в потоке:

- Идентификация потока: протокол, src/dst IP/порт...
- Число пакетов
- Число байт
- Время начала и окончания потока
- Может быть, дополнительная информация, например номера автономных систем (AS), сетевые маски

Сохраняет объем и тип трафика, но не его *содержимое*

Использование и приложения

Возможность отвечать на такие вопросы:

- Какой пользователь / отдел скачивал / закачивал больше всего?
- Какие протоколы используются в сети чеще всего?
- Какие устройства создают самый большой трафик SMTP, и куда?

•Обнаружение атак и аномалий

•Более детальная визуализация (графики), чем может быть сделано на уровне

Работа с потоками

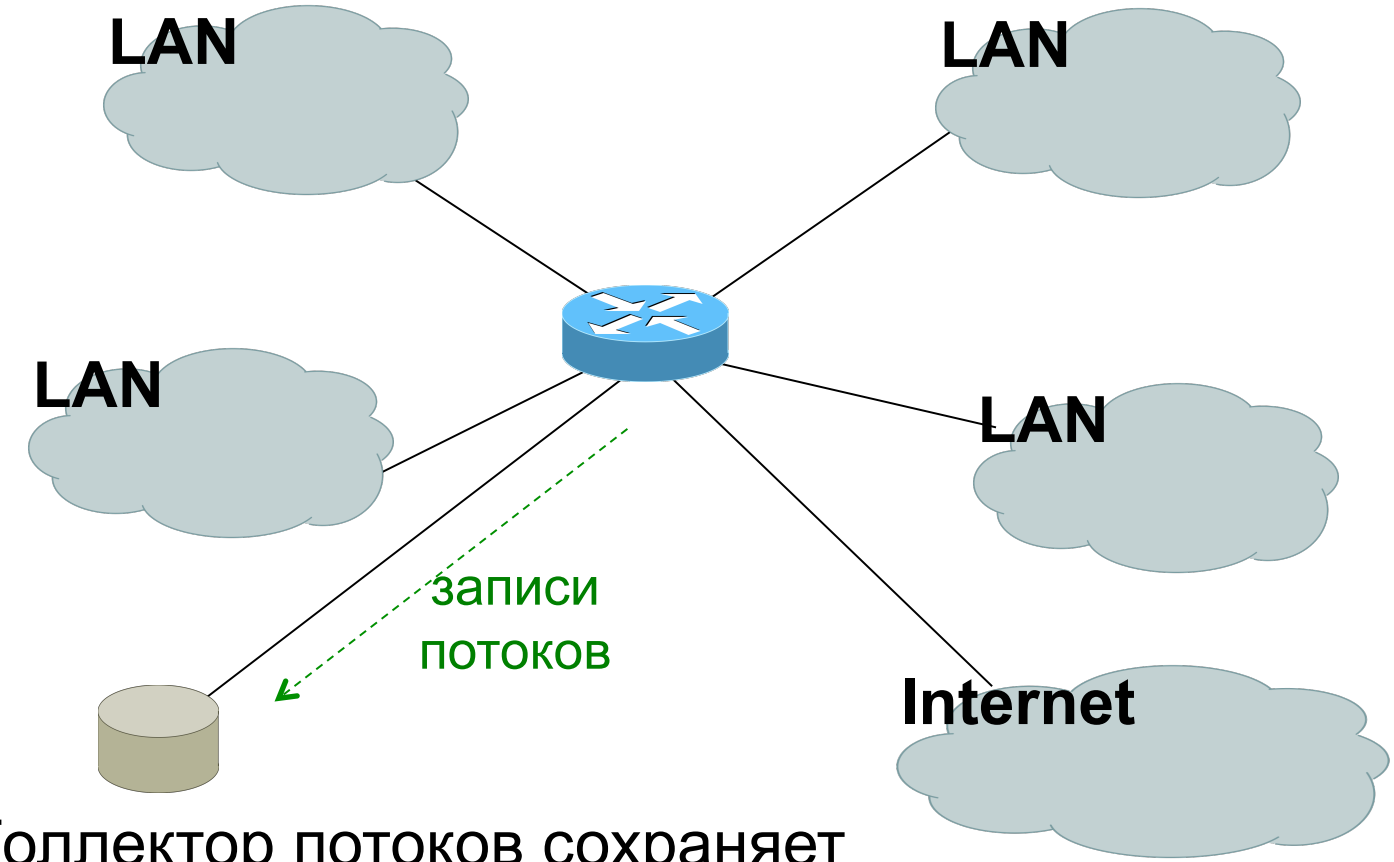
1. Настроить устройство (например, роутер) создавать записи учета потоков
2. Экспортировать потоки с устройства (роутера) на коллектор (PC)
   - Настроить получателя и версию протокола
3. Получать потоки, сохранять их на диске
4. Анализировать потоки

Много доступных инструментов, бесплатных и платных

Где создавать записи потоков

1. На роутере или другом сетевом устройстве
   - Если устройство это поддерживает
   - Не требуется дополнительное оборудование
   - Может влиять на производительность
2. Пассивный коллектор (обычно Unix сервер)
   - Получает копию каждого пакета и создает потоки
   - Требует зеркалированного порта

Сбор потоков с роутера

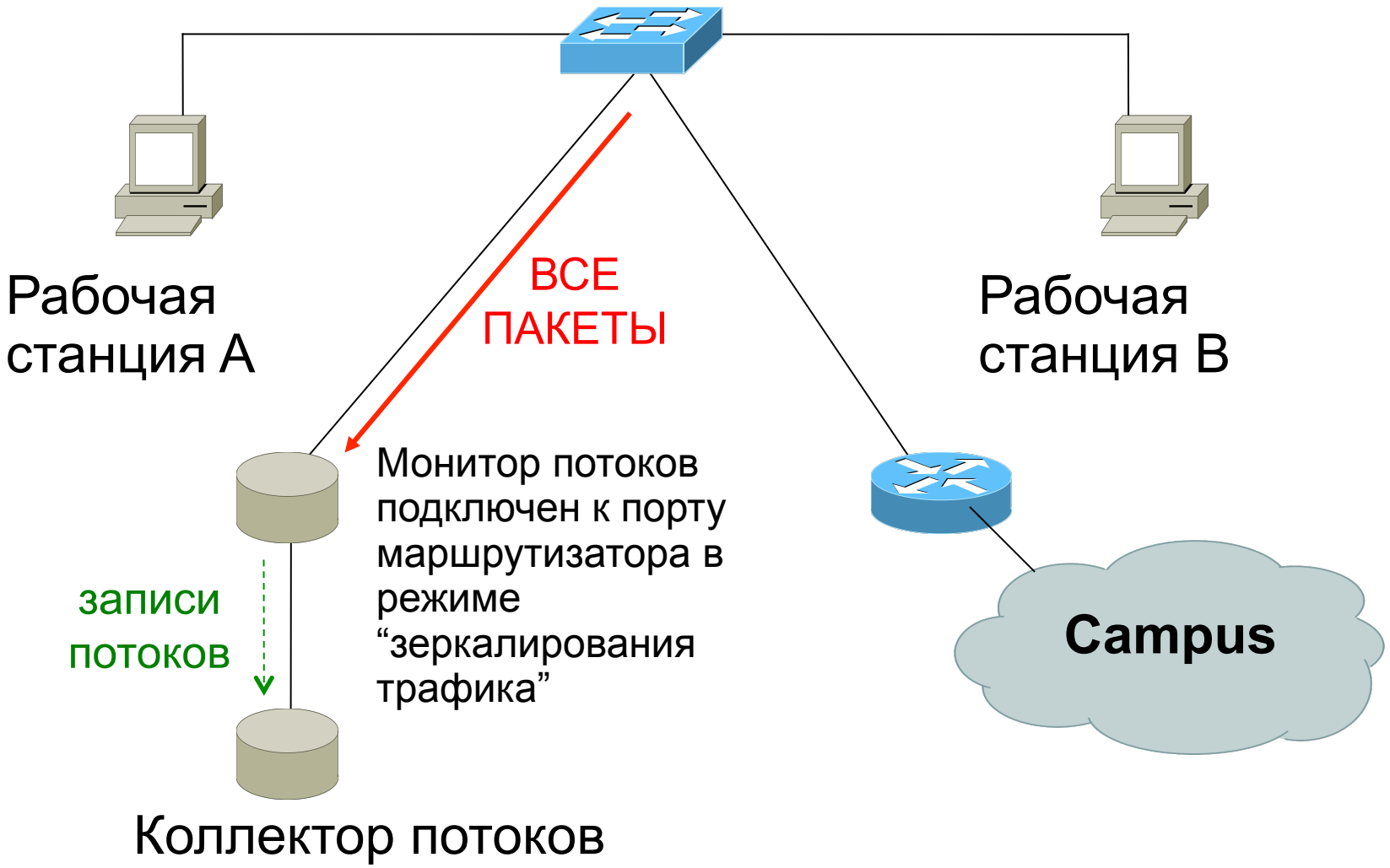


Коллектор потоков сохраняет экспортированные роутером потоки.

Сбор потоков с роутера

- Все потоки через роутер могут отслеживаться
- Накладные расходы ресурсов роутера для обработки и экспорта потоков
- Можно выбрать, для каких интерфейсов сбор потоков нужен и не активировать его на других
- Если в каждой LAN есть свой роутер, можно активировать Netflow на них, с целью уменьшения нагрузки на основной

Пассивный коллектор



Пассивный коллектор

Примеры

- softflowd (Linux/BSD)
- pfflowd (BSD)
- ng_netflow (BSD)

•Коллектор видит весь трафик через точку в сети, к которой он подсоединен и создает потоки

•Освобождает роутер от нагрузки, связанной с обработкой трафик, создания и экспорта потоков

Пассивный коллектор, прод.

Полезно на соединениях:

- с одной точкой входа в сеть
- где нужны только потоки от одной части сети

Может быть размещен совместно с IDS

Идея:

В вашей сети наверное уже есть устройство, отслеживающее IP адреса и номера портов трафика, текущего через него.

Что это за устройство?

Протоколы экспортирования потоков

- Cisco Netflow, разные версии
  - v5: широко используется
  - v9: более новый, расширяемый, включает поддержку IPv6
- IP Flow Information Export (**IPFIX**):
  - стандарт IETF, основан на Netflow v9
- **sFlow**: работает с выборкой пакетов, обычно реализуется на коммутаторах
- **jFlow**: Juniper
- Мы пользуемся Netflow; многие

Cisco Netflow

- Однонаправленные потоки
- IPv4 unicast и multicast
  - (IPv6 в Netflow v9)
- Протоколы экспортируются через UDP
  - Выберите порт. Стандарта нет, хотя часто используются 2055 и 9996
- Поддерживается IOS, ASA и CatOS, но реализации отличаются

Конфигурация Cisco IOS

- Настраивается для каждого входящего интерфейса
  - современные IOS позволяют отслеживать и входящий и исходящий трафик
- Задайте версию
- Задайте адрес и порт коллектора (куда отправлять потоки)
- Опционально, разрешите таблицы агрегации
- Опционально, настройте таймаут потока и размер главной таблицы потоков (v5)

Конфигурация Netflow: старый метод

Активируйте CEF

- `ip cef`
- `ipv6 cef`

Активируйте потоки на каждом интерфейсе

```
ip route cache flow
ИЛИ
ip flow ingress
ip flow egress
```

Экспортируйте потоки в коллектор

```
ip flow-export version [5|9] [origin-as|peer-as]
ip flow-export destination <x.x.x.x> <udp-port>
```

"Гибкий Netflow": новый метод

- Единственный способ отслеживания потоков IPv6 на современных IOS
- Используйте его – IPv6 грядет / уже здесь
- Много странных параметров настройки, хотя базовай конфигурация достаточно прямолинейна

Гибкая конфигурация netflow

- Задайте один или более экспортеров

```
flow exporter EXPORTER-1
 destination 192.0.2.99
 transport udp 9996
 source Loopback0
 template data timeout 300
```

- Задайте один или более мониторов потоков

```
flow monitor FLOW-MONITOR-V4
 exporter EXPORTER-1
 cache timeout active 300
 record netflow ipv4 original-input
flow monitor FLOW-MONITOR-V6
 exporter EXPORTER-1
 cache timeout active 300
 record netflow ipv6 original-input
```

Гибкая конфигурация netflow

Назначьте мониторы потоков интерфейсу

```
interface GigabitEthernet0/0/0
 ip flow monitor FLOW-MONITOR-V4 input
 ip flow monitor FLOW-MONITOR-V4 output
 ipv6 flow monitor FLOW-MONITOR-V6 input
 ipv6 flow monitor FLOW-MONITOR-V6 output
```

Наиболее активные пользователи

Вы можете получить сводку потоков прямо на роутере, например

```
show flow monitor FLOW-MONITOR-V4
cache aggregate ipv4 source address
ipv4 destination address sort
counter bytes top 20
```

И да, это одна длинная команда!

Старая команда "show ip flow top-talkers", к сожалению, не поддерживается, но можно сделать алиас:

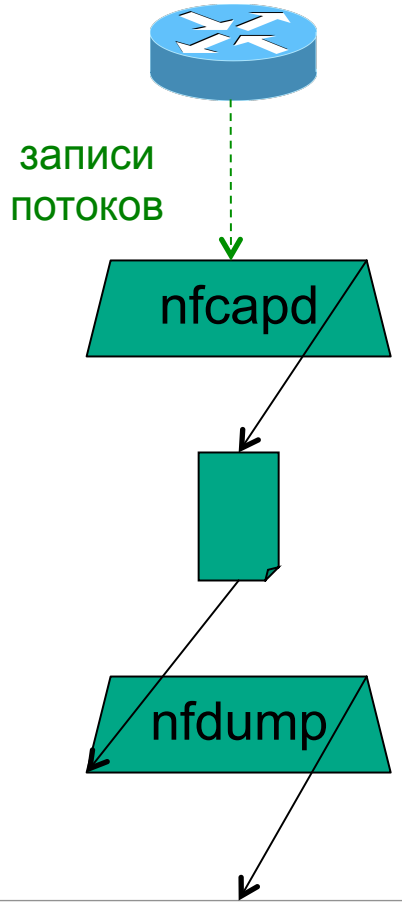
```
-conf t
 alias exec top-talkers show flow
```

Вопросы?

Сбор потоков: nfdump

- Бесплатный и открытый – запускается на коллекторе
- *nfcapd* получает входящие записи потоков и сохраняет их на диске (просто в файлах)
  - обычно создает новый файл каждые 5 минут
- *nfdump* читает файлы и конвертирует их в форму, удобную для чтения человеком
- У nfdump есть параметры для фильтрования и агрегирования потоков

Архитектура nfdump



программа-демон

файлы

командная строка

```
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2013-04-18 13:35:23.353  1482.000 UDP        10.10.0.119:55555 ->   190.83.150.177:54597     8683   445259     1
2013-04-18 13:35:23.353  1482.000 UDP      190.83.150.177:54597 ->     10.10.0.119:55555     8012   11.1 M     1
2013-04-18 13:48:21.353   704.000 TCP       196.38.180.96:6112  ->     10.10.0.119:62099       83    20326     1
2013-04-18 13:48:21.353   704.000 TCP        10.10.0.119:62099 ->    196.38.180.96:6112       105     5085     1
```

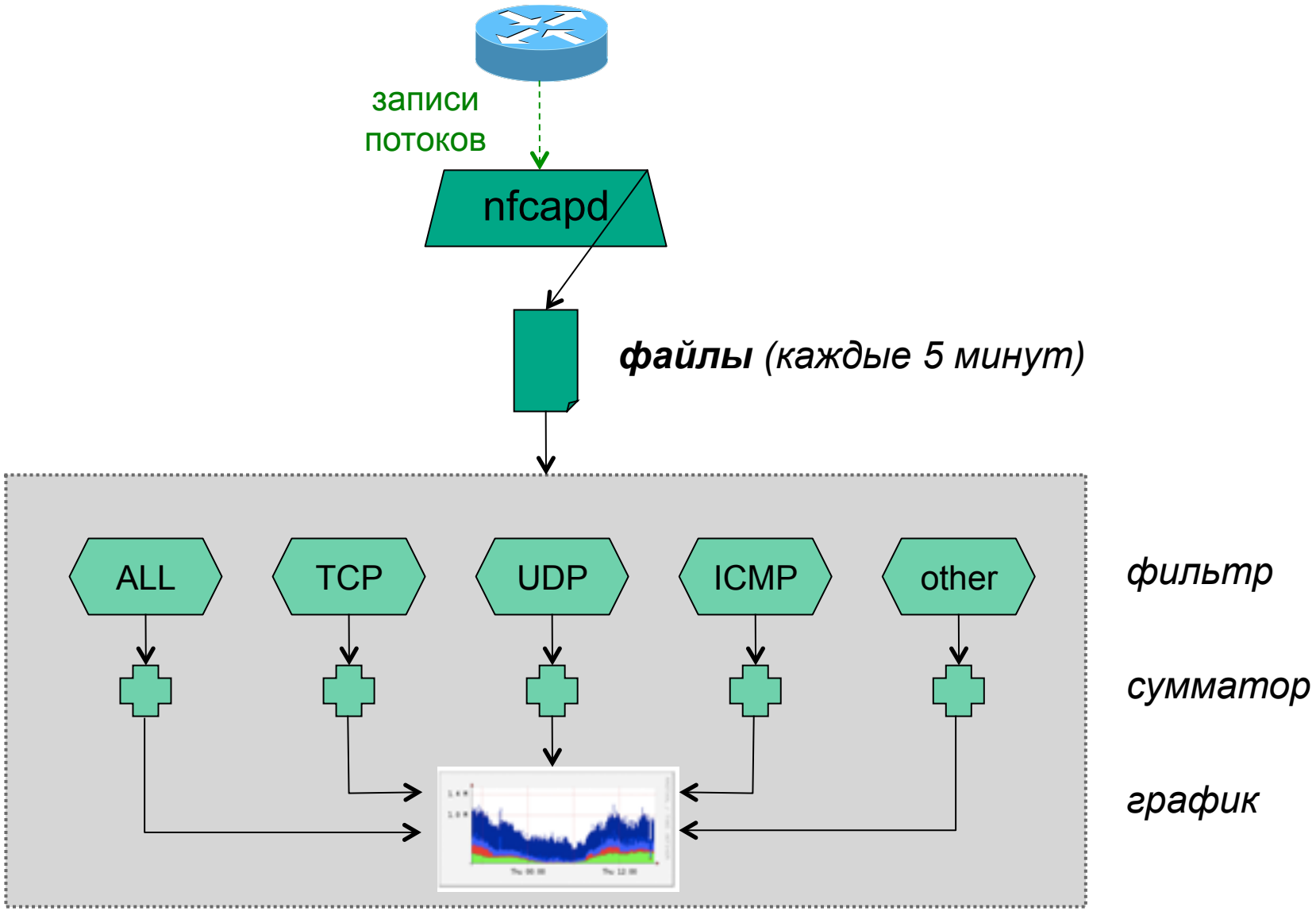
Анализ потоков: nfsen

- Используется вместе с nfdump
- Web-интерфейс
- Создает графики трафика (RRD)

Позволяет выбрать интересующее время и сделать анализ нужного интервала с помощью nfdump

- Управляет процессами nfcapd
  - Может запускать несколько nfcapd для получения потоков от разных роутеров
- Доступны такие плагины как port tracker,

Архитектура nfsen



nfsen: замечания

- Каждые 5 минут nfcapd начинает новый файл, и nfsen обрабатывает предыдущий
- Следовательно, каждая точка на графике соответствует 5-минутному интервалу
- График показывает *сумму* выбранного трафик в этот 5-минутный период
- Чтобы получить более детальную информацию о индивидуальных потоках

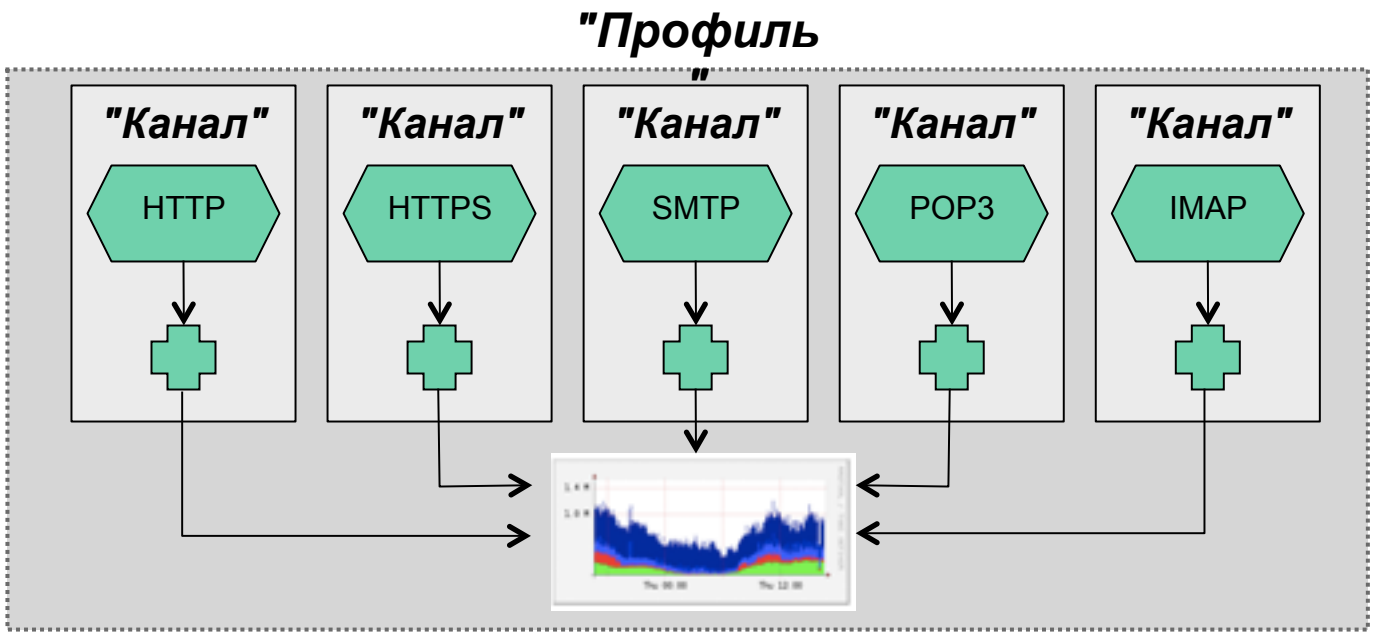
Демонстрация

Мы будет использовать nfsen чтобы найти самых больших потребителей пропускной способности

Профили и каналы

- "Канал" определяет, график какого типа трафика строить, и “профиль” - это набор каналов, которые можно показать вместе
- Вы можете создать ваши собственные профили и каналы, и следовательно графики, например
  - Общий HTTP, HTTPS, SMTP трафик (и т.д.)
  - Трафик из научного отдела и в него
  - ...
- Пользуйтесь фильтрами для

Профили и каналы



фильтр

сумматор

график

Ссылки – инструменты

nfdump и nfsen:

http://nfdump.sourceforge.net/
http://nfsen.sourceforge.net/
http://nfsen-plugins.sourceforge.net/

pmacct и pmgraph:

http://www.pmacct.net/
http://www.aptivate.org/pmgraph/

flow-tools:

http://www.splintered.net/sw/flow-tools

Ссылки – дальнейшая информация

- WikiPedia:
  http://en.wikipedia.org/wiki/Netflow
- Стандарты IETF:
  http://www.ietf.org/html.charters/ipfix-charter.html
- Страница NetFlow Abilene
  http://abilene-netflow.itec.oar.net/
- Cisco Centric Open Source Community
  http://cosi-nms.sourceforge.net/related.html
- Документация пользователя Cisco NetFlow коллектора
  http://www.cisco.com/en/US/docs/net_mgmt/netflow_collection_engine/6.0/tier_one/user/guide/user.html

Конец

(Далее следует дополнительный справочный материал)

Примеры фильтров

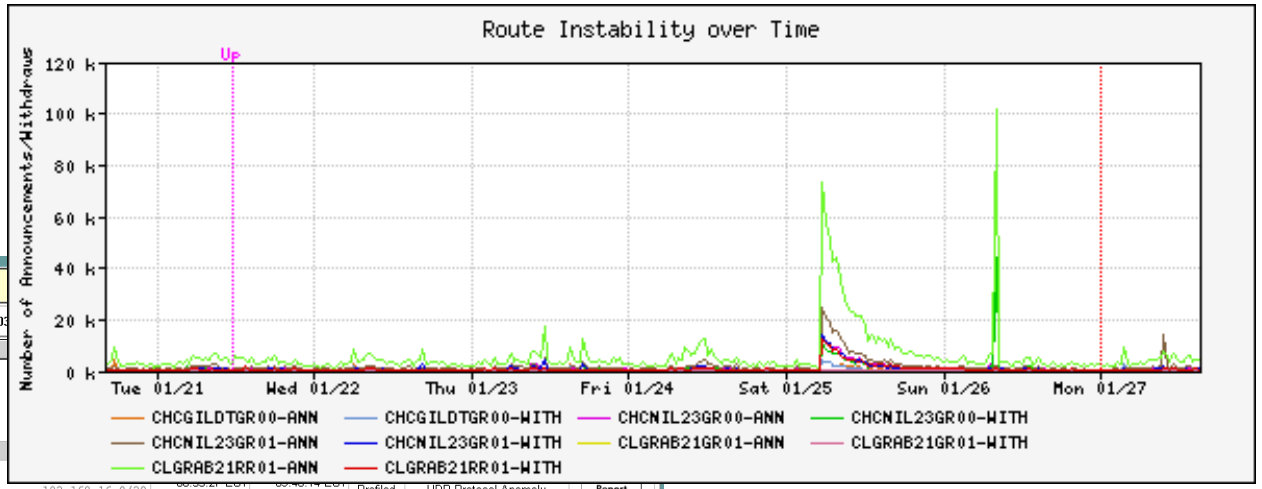
any	*весь трафик*
proto tcp	только *TCP*
dst host 1.2.3.4	только трафик к *1.2.3.4*
dst net 10.10.1.0/24	только трафик в эту сеть
not dst net 10.10.1.0/24	только трафик не в эту сеть
proto tcp and src port 80	только TCP с *only портом отправителя 80*
dst net 10.10.1.0/24 or dst net 10.10.2.0/24	*только трафик в эти сети*
dst net 10.10.1.0/24 and proto tcp and src port 80	только ответы *HTTP в эту сеть*
(dst net 10.10.1.0/24 or dst net 10.10.2.0/24) and proto tcp and src port 80	...возможны более сложные комбинации

Потоки и приложения: Больше примеров

Использование NetFlow

- Нахождение и решение проблем
  - Классификация трафика
  - Отслеживание DoS (слайды от Danny McPherson)
- Анализ трафика
  - Анализ трафика между AS
  - Отчеты о прокси приложений
- Учет (и биллинг)
  - Перекрестная проверка из других источников
  - Можно сравнивать с данными SNMP для проверки

Обнаружение аномалий: червяк SQL “Slammer”*



peakflow DoS

Recent Anomalies : Anomaly 125772 : Detailed Statistics

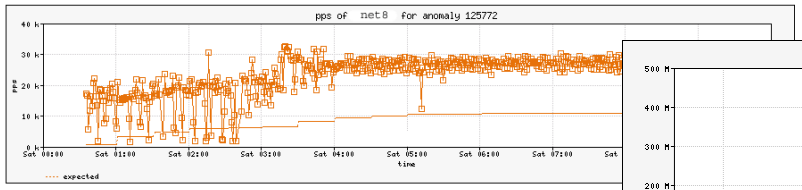
11:51:49 EST 27 Jan 2003

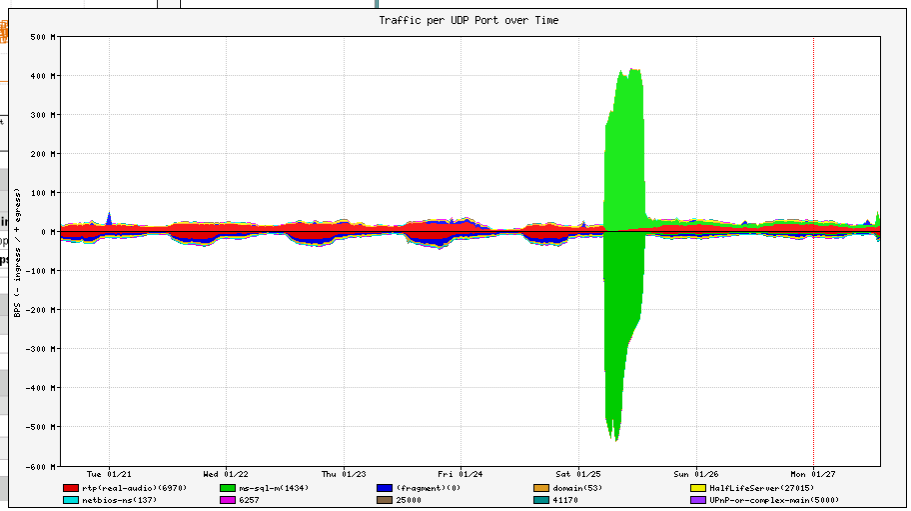
Status | Topology | Ongoing | Recent | Dark IP | Admin | About

Anomaly 125772 Detailed Statistics

ID	Importance	Severity	Duration	Direction
125772	High	958.2% of 3.40 Kpps	09h 06m 47s	Outgoing

192.168.16.0/20 members_misc_nets	25 Jan 2003	25 Jan 2003	Profiled	UDP Protocol Anomaly





Affected Network Elements

Router net8 1.2.3.4

	Triggering	Expected	Difference	Maxi
Bitrate	71.69 Mbps	2.34 Mbps	69.35 Mbps	105.26 Mbp
Packet Rate	**22.20 Kpps**	**712 pps**	**21.49 Kpps**	**32.58 Kpp**

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Summary of all Data Snapshots Collected:

	Bytes	Packets	Bytes/Pkt	bps
	308.01 GB	762,849,500	404 B	76.05 Mbps

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Source Addresses

Network / Mask	Bytes	▼Packets	Bytes/Pkt	bps
192.168.20.217/32	168.22 GB	416,436,800	404 B	41.54 Mbps
192.168.18.187/32	139.53 GB	345,372,800	404 B	34.45 Mbps

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Destination Addresses

Обнаружение аномалий (прод.)*

Когда база известна, получается обнаруживать аномальную активность

- Обычные аномалии **основанные на скорости** (пакеты в секунду или биты в секунду) могут быть безвредными либо вредоносными
- Многие **злоупотребления** могут быть немедленно обнаружены, даже **без** базовых значение (TCP SYN или потоки RST)
- **Подписи** также могут определяться для идентификации “интересных” потоков (например, proto udp and port 1434 and 404 octets(376 payload) == slammer!)
- Сложные временные подписи могут использоваться для обнаружения аномалий с высокой точностью

Платные продукты…*

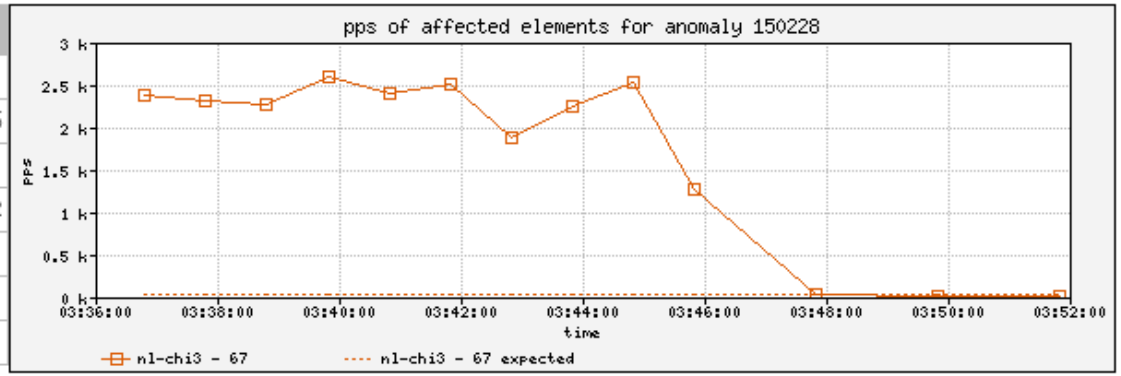
Anomaly 150228

Get Report: PDF XML

ID	Importance	Duration	Start Time	Direction	Type	Resource
150228	High 130.0% of 2 Kpps	17 mins	03:34, Aug 16	Incoming	Bandwidth (Profiled)	Microsoft 207.46.0.0/16 windowsupdate.com

Traffic Characterization

Sources	204.38.130.0/24
	204.38.130.192/26
	1024 - 1791
Destination	207.46.248.234/32
	80 (http)
Protocols	tcp (6)
TCP Flags	S (0x02)

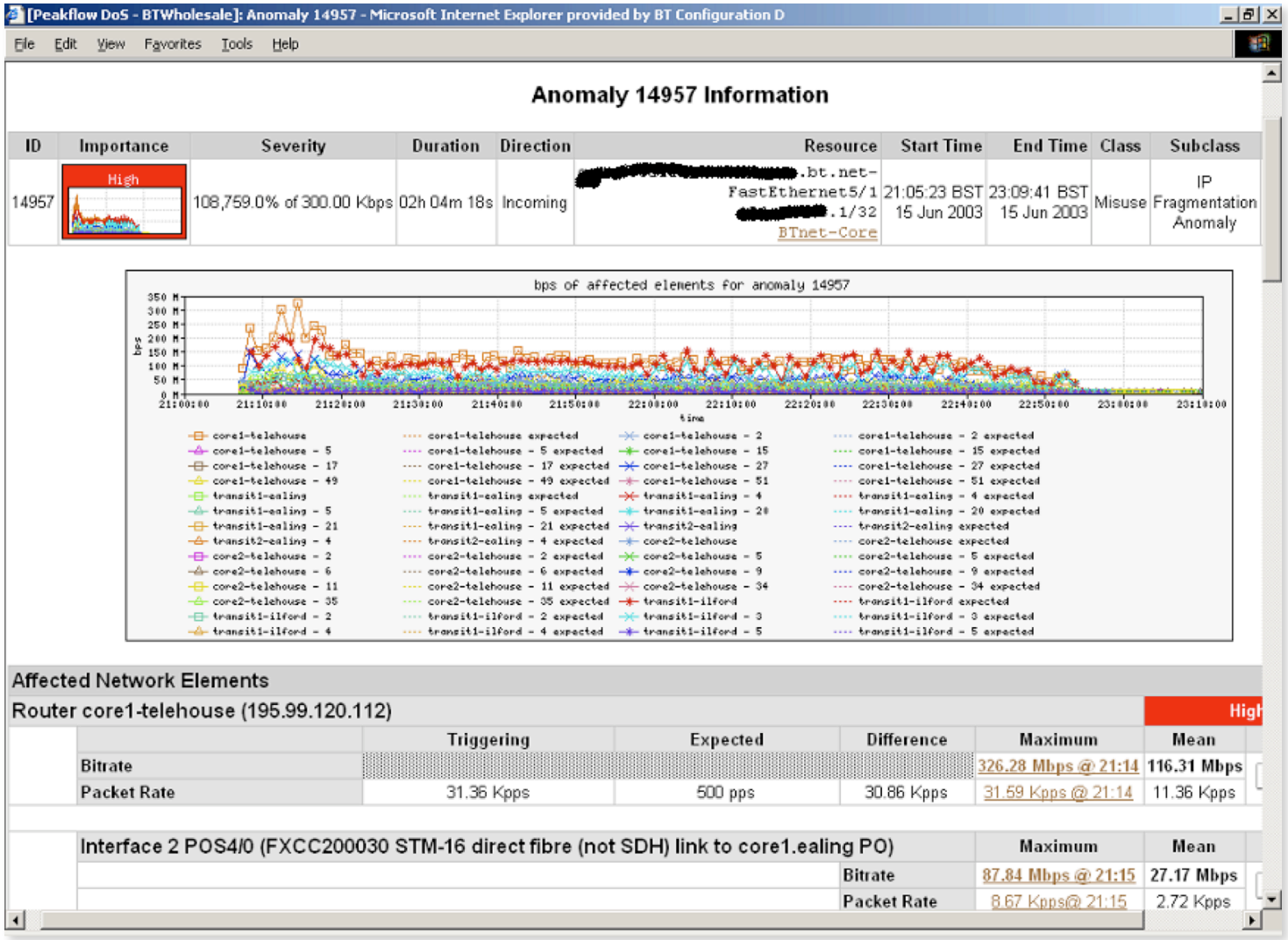


Affected Network Elements

	Importance	Expected pps	Observed bps Max	Observed bps Mean	Observed pps Max	Observed pps Mean	
Router nl-chi3 198.110.131.125	High						
Interface 67 at-1/1/0.14 *pvc to WMU*		26	832 K	563.1 K	2.6 K	1.7 K	Details

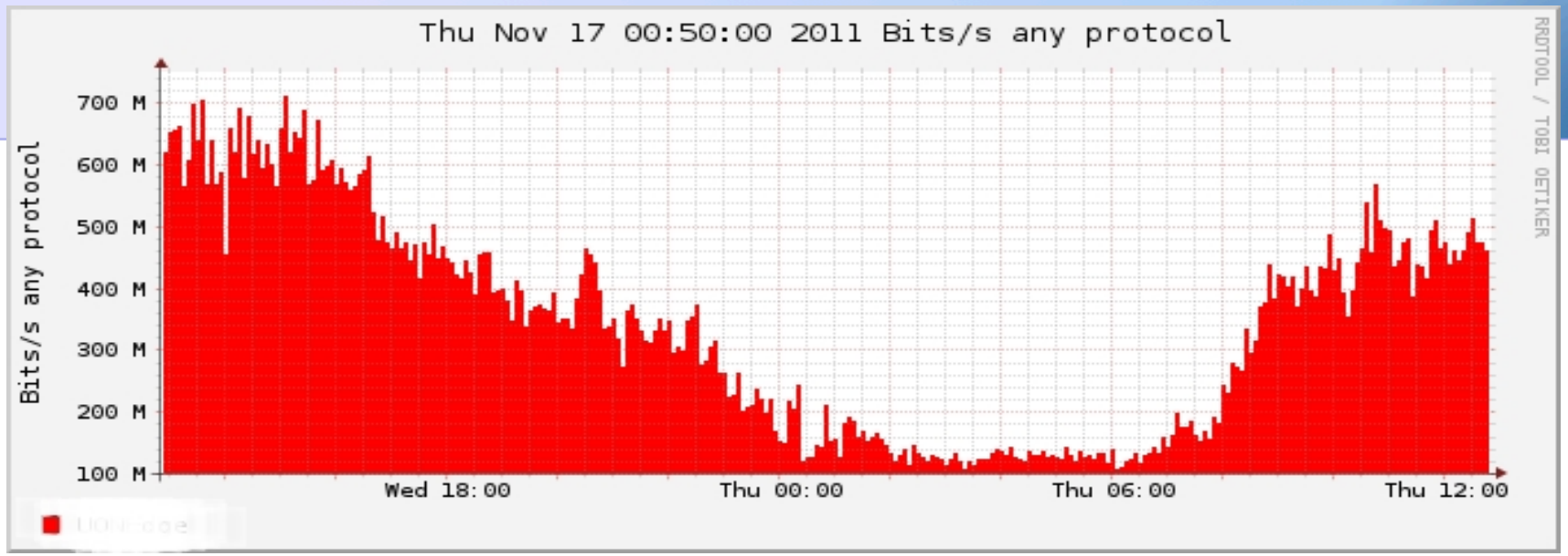
Anomaly Comments

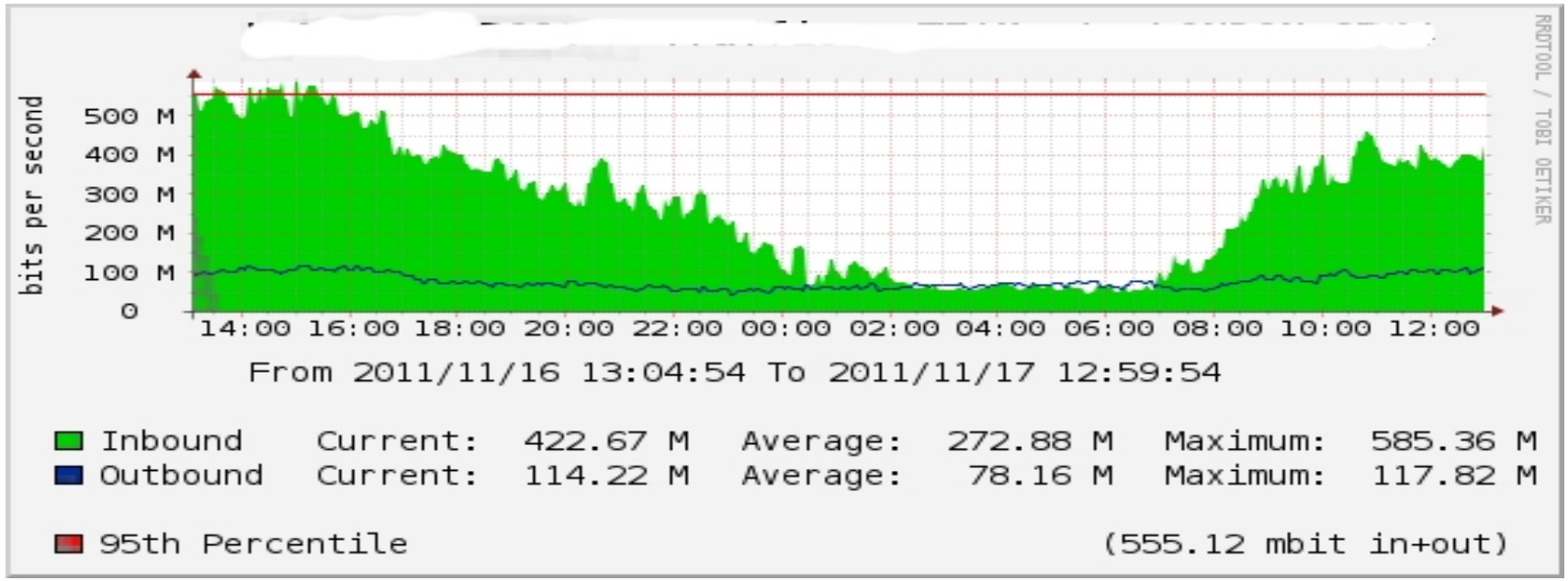
Обнаружение платным продуктом: широкомасштабная атака DOS



Учет

Учет, основанный на потоках может быть хорошим дополнением к учету, основанному на SNMP.


Thu Nov 17 00:50:00 2011 Bits/s any protocol
Bits/s any protocol
700 M
600 M
500 M
400 M
300 M
200 M
100 M
Wed 18:00
Thu 00:00
Thu 06:00
Thu 12:00
RRDTOOL / TOBI OETIKER


bits per second
500 M
400 M
300 M
200 M
100 M
0
14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00
From 2011/11/16 13:04:54 To 2011/11/17 12:59:54
Inbound Current: 422.67 M Average: 272.88 M Maximum: 585.36 M
Outbound Current: 114.22 M Average: 78.16 M Maximum: 117.82 M
95th Percentile (555.12 mbit in+out)
RRDTOOL / TOBI OETIKER

Версии Cisco Netflow

NetFlow версии 1

- Ключевые поля: IP и порты отправителя/получателя, протокол IP, ToS, входящий интерфейс.
- Учет: пакеты, байты, время начала/ конца, исходящий интерфейс
- Другое: побитный ИЛИ флагов TCP.
- Не имеет последовательных номеров – нельзя определить потерянные потоки
- Устаревший

NetFlow Versions 2-4

- Внутренние для Cisco
- Никогда не были выпущены

NetFlow v5

- Ключевые поля: IP и порты отправителя/получателя, протокол IP, ToS, входящий интерфейс.
- Учет: пакеты, байты, время начала/конца, исходящий интерфейс
- Другое: побитный ИЛИ флагов TCP, AS отправителя/получателя, сетевая маска
- Формат пакета добавляет последовательные номера для обнаружения потерянных потоков
- Только IPv4

NetFlow v8

- Агрегирование потоков v5.
- Не все типы потоков доступны на всем оборудовании
- Намного меньше данных для обработки, но теряет детальность версии 5 – нет адресов IP.

NetFlow v9

- Поддержка IPv6
- Дополнительные поля, например метки MPLS
- Расширяет предыдущие версии
- Периодически отправляет пакет “шаблона”, все поля данных потоков ссылаются на шаблон
- Может экспортироваться по TCP