Gigamon®

Gigamon. Копирование и фильтрация трафика. Часть 3

Александр Грачев

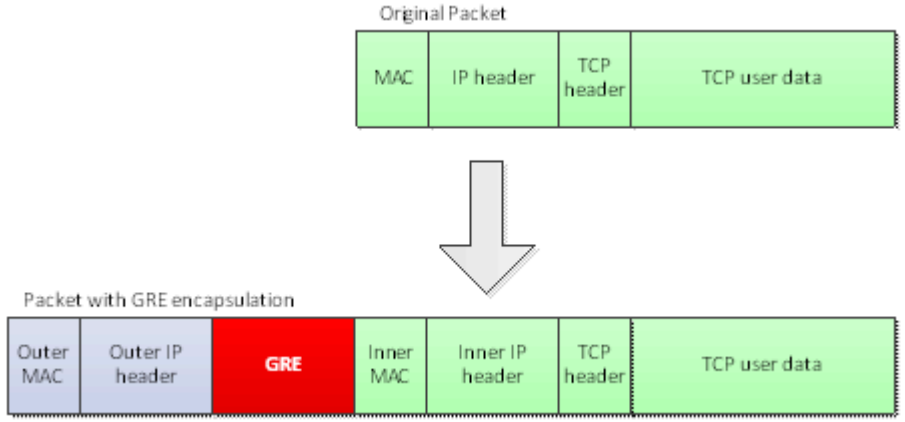
Менеджер по развитию бизнеса
Нетвелл

Tunneling

- Получение копии трафика от виртуальных решений Гигамон (GigaVUE-VM/V-Series nodes).
- Передача копий трафика между Гигамонами по IP сети.
- Получение копии трафика от сетевых устройств и виртуальных свичей через ERSPAN v2 и v3/VXLAN
- Поддержка IPv4 и IPv6

Что такое L2GRE и GMIP

- GRE или Generic Routing Encapsulation, простой протокол тунелирования добавляющий к оригинальному свой заголовок. Работает **IPV4/IPV6+UDP.**
- L2GRE или Network visualized GRE (NVGRE) разновидность инкапсуляции **"Mac-in-IP"**, позволяющая «упаковать» Ethernet пакет в L3 тоннель. Т.о. после заголовка тоннеля в таком пакете будет идти заголовок Ethernet оригинального пакета
- GMIP аналог L2GRE разработанный Gigamon. Протокол простого туннелирования использующий UDP заголовки в качестве инкапсуляции.



Туннелирование без GigaSMART (L2GRE/VXLAN)

- Отправка\прием трафика через VXLAN или L2GRE на полной скорости всех портов.
- Не загружается GigaSMART модуль
- Поддерживаемые платформы HC1/HC2 (только CCv2)/HC3/TA40/TA100/TA200
- Для использования на TA-серии требуется лицензия Advanced feature
- Удобный инструменты для передачи копий трафика через IP сеть, как между устройствами Gigamon, так и конечному получателю
- В map выполняется фильтрация по внутренним заголовкам пакета (так же по GRE-ID, и внешнему VLAN)
- Только в map by rule
- При отправки трафика в тоннель network порт нельзя использовать в map-passall
- Нельзя использовать операции GigaSMART
- Не поддерживается IPv6
- Не более 1500 GRE-ID\VXLAN на шасси.
- Обязательно наличие в GRE-ID в принимаемом трафике.

Туннелирование с GigaSMART (L2GRE/GMIP)

- Отправка\прием трафика через GMIP или L2GRE тоннели используя ресурсы GigaSMART для инкапсуляции\декапсуляции.
- Декапсуляция следующих протоколов ERSPAN, VXLAN, GMIP. Так же предусмотрена настриваема терминация тоннелей, или прием чистой копии трафика на IP интерфейс.
- Т.к. удаление заголовка происходит на модуле GigaSMART, поэтому правила фильтрации в MAP будут применяться к заголовку тоннеля.
- Базовая лицензия GigaSMART позволяет только терминировать GMIP тоннели, например от GigaVUE-VM или V-Series node.
- Позволяет терминировать GRE и ERSPAN, без указания flow-id или вообще без flow-id. GigaVUE-VM отправляет копию трафика без GRE-ID, поэтому для приема такой копии трафика необходимо только GigaSMART туннелирование.

Туннелирование без GigaSMART L2GRE – настройка инкапсуляции

1. Исходящему порту назначаем тип Circuit C
2. Назначаем GRE-ID который будет использован при инкапсуляции (он может быть один на шасси)
3. Создаем IP Interface для этого порта
4. Создаем туннель. В нем указываем именно название IP Interface, а не физического порта
5. Создаем карту фильтрации где в качестве исходящего порта указываем название тоннеля

Пример конфигурации

```
port 7/1/x3 type circuit
port 7/1/x3 params admin enable

tunnel l2gre box-id 7 global-encap-id 5

ip interface alias IP-INT-circuit
  attach 7/1/x3
  ip address 3.3.3.1 /30
  gw 3.3.3.2
  exit

tunnel alias tunnel-gre-1-enc encap l2gre
  attach IP-INT-circuit
  ipdst 3.3.3.2
  exit

map alias test-gre-6
  rule add pass ipver 4
  to tunnel-gre-1-enc
  from 7/1/x6
  exit
```

Gigamon

Туннелирование без GigaSMART L2GRE – настройка декапсуляции

1. Входящему порту назначаем тип Circuit C
2. Прописываем список GRE-ID, которые будут терминироваться на устройстве (не более 1500 на шасси)
3. Создаем IP Interface для этого порта
4. Создаем туннель. В нем указываем именно название IP Interface, а не физического порта
5. Создаем карту фильтрации где в качестве входящего порта указываем название IP Interface

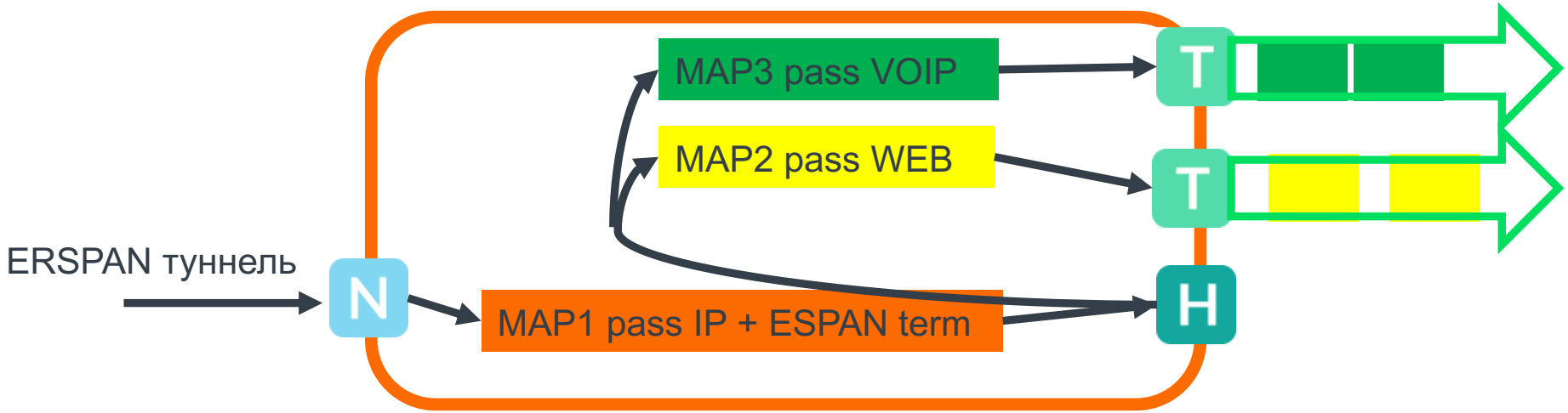
Пример конфигурации

```
port 7/1/x4 type circuit
port 7/1/x4 params admin enable

tunnel l2gre box-id 7 l2gre-group alias test-gre-group
  add 5
  exit

ip interface alias test-2-circuit
  attach 7/1/x4
  ip address 3.3.3.2 /30
  gw 3.3.3.1
  exit

tunnel alias test-gre-2-dec decap l2gre
  attach test-2-circuit
  exit

map alias test-gre-6-dec
  rule add pass ipver 4
  to 7/1/x9
  from test-2-circuit
  exit
```

Gigamon

Tunneling. Конфигурирование.

1) Создаем IP Interface. Назначаем ему IP Адрес, шлюз по умолчанию, MTU и привязываем его к нужной Gigasmart group
2) Создаем GigaSMART операцию.
3) Создаем MAP-Byrule с GigaSMART операцией.
4) !!!!ВНИМАНИЕ!!!! Т.к. Сам заголовок тоннеля будет удален только на модуле GigaSMART, то MAP, в которой будет применена GSOP терминации тоннеля, будет выполнять фильтрацию по заголовку этого тоннеля, а не по заголовку пакета находящегося внутри. Поэтому для фильтрации полученной копии трафика, в MAP с «тоннельной» GSOP нужно указать порт-получатель Hybrid. А затем создавать карту в которой этот порт будет источником и выполнять фильтрацию.



NetFlow / IPFIX /CEF Generation

- Генерирует Netflow\IPFIX из копии трафика, которая есть на платформе.
- Если устройство в кластере отправляющий порт может располагаться на удаленном устройстве, не на том где есть модуль GigaSMART
- Поддерживаемые версии Netflow V5, Netflow V9, IPFIX+Метаданные
- Передача метаданных через CEF.
- Возможность генерирования NetFlow группой модулей GigaSMART, позволяет масштабировать производительность платформы.
- Генерация Netflow из IPv4 и IPv6 трафика, но передача коллектору только по IPv4
- Возможность передачи Netflow нескольким коллекторам-получателям

IPFIX расширенные метаданные

GigaSMART NetFlow Generation позволяет обогащать IPFIX информационными элементами верхних уровней. Их анализ позволяет контролировать работу сервисных платформ, а так же выявлять сложные высокоуровневые атаки и вредоносные активности в сети.

Доступные дополнительные информационные элементы:

Extension	Example Metadata
DNS	RDATA, Query Name, OPCODE, AXFR/IXFR (40+ информационных элементов)
HTTP	URLs, GET, POST, PUT, DELETE, and HEAD method types, ALL 2xx 3xx 4xx 5xx Коды ответов
SIP	INVITE, ACK, BYE, REGISTER, OPTIONS, and CANCEL типы запросов
Certificates	Cert Subject, SNI, Cert Issuer, Issue date (20+ информационных элементов)

NetFlow и IPFIX. Конфигурирование.

1 Exporter

- Получатель Netflow
- Конфигурируем в GigaSMART->Netflow

2 IP Interface

- Порт отправитель, должен быть Tool
- Конфигурируем в Ports-> IP Interfaces

3 Record

- Какую статистику собираем и версия Netflow
- Конфигурируем в GigaSMART->Netflow

4 Monitor

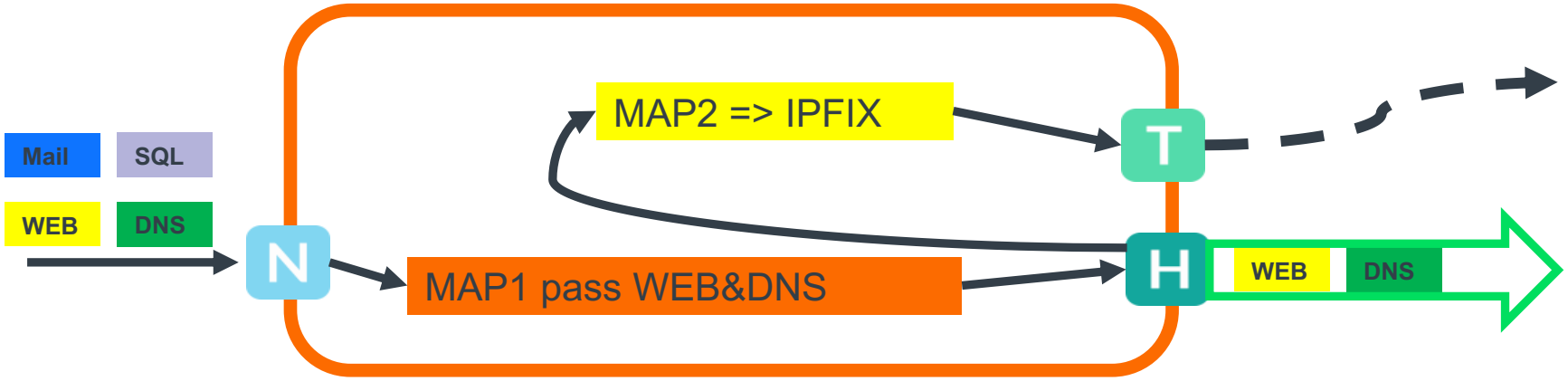
- Как формируем статистику
- Конфигурируем в GigaSMART->Netflow

5 Monitor-GSGROUP

- Привязываем Monitor к Gigasmart Group.
- Конфигурируем в GigaSMART->GigaSMART Groups

6-7 GSOP-MAP

- Создаем GigaSMART операцию
- Создаем MAP-ByRule с GigaSMART операцией



Внимание:

Часто бывает так, что нам нужно отправлять трафик в «сыром» виде одним получателям и из него же сгенерировать NetFlow для других получателей. Одно из решений этой задачи приведено на рисунке слева

Gigamon®

Благодарю за внимание!