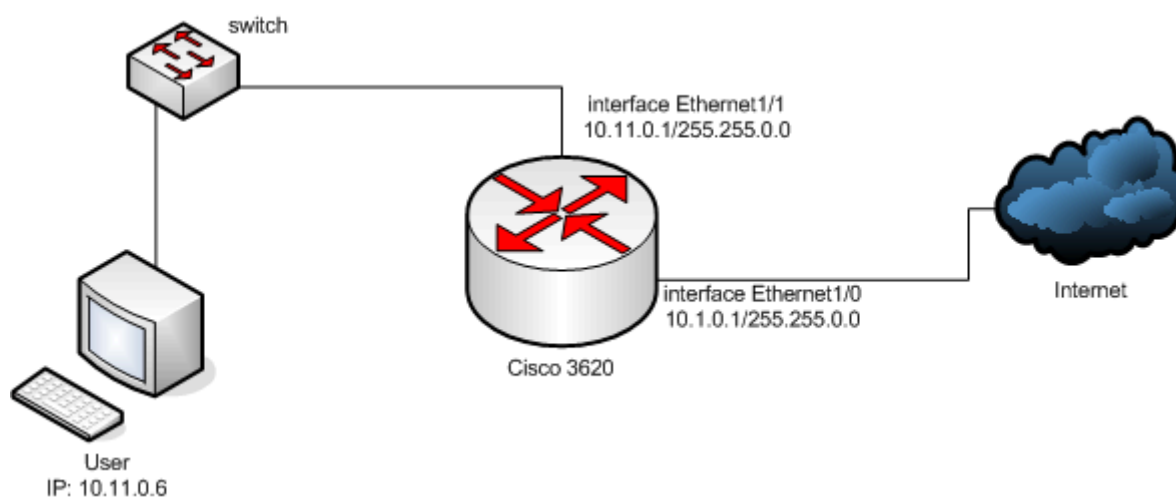


Сбор статистики по протоколу Netflow с маршрутизатора Cisco в случае использования NAT.

Основная проблема при использовании Netflow совместно с технологией преобразования IP-адресов - NAT, заключается в том, что на внутреннем интерфейсе будет фиксироваться информация о переданном от клиента трафике, а на внешнем интерфейсе будет фиксироваться трафик, переданный из сети Интернет на внешний IP-адрес маршрутизатора. Таким образом, в Netflow потоке будет информация о переданном трафике от клиента, но не будет фигурировать информация о данных переданных в сторону клиента. Например, в рассмотренном ниже конфигурационном файле внутренняя сеть имеет IP-адреса 10.11.0.0 маска подсети 255.255.0.0, а внешний интерфейс маршрутизатора имеет IP-адрес 10.1.0.1. При этом пользователь 10.11.0.6 пытается загрузить страницу www.netup.ru с IP-адресом 195.161.112.6.



Ниже приводится конфигурационный файл маршрутизатора Cisco с комментариями:

```
Current configuration : 4013 bytes
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Router  
!  
boot-start-marker  
boot-end-marker  
!  
ip subnet-zero  
!  
ip cef  
!
```

Интерфейс, на который производится перенаправление пакетов после обратного преобразования. Таким образом, на данном интерфейсе будет проходить трафик с IP-адреса 195.161.112.6 на IP-адрес 10.11.0.6. Что бы данный трафик экспортировался по Netflow, указываем опцию `ip route-cache flow`.

```
!  
interface Loopback0  
ip address 192.168.10.1 255.255.255.0  
ip route-cache policy  
ip route-cache flow  
!
```

Внешний интерфейс маршрутизатора. На данном интерфейсе проходит трафик с IP-адреса 195.161.112.6 на IP-адрес этого же интерфейса – 10.1.0.1. Что бы данный трафик экспортировался по NetFlow, указываем опцию `ip route-cache flow`.

Так же на данном интерфейсе необходимо указать опцию `ip policy route-map MAP`, что бы пакеты после обратного преобразования направлялись на интерфейс Loopback 0 согласно правилам, указанным в `route-map`.

```
!  
interface Ethernet1/0  
 ip address 10.1.0.1 255.255.0.0  
 ip nat outside  
 ip route-cache policy  
 ip route-cache flow  
 ip policy route-map MAP  
!
```

Внутренний интерфейс маршрутизатора. На данном интерфейсе проходит трафик с IP-адреса клиента – 10.11.0.6 на IP-адрес 195.161.112.6. Что бы данный трафик экспортировался по NetFlow, указываем опцию `ip route-cache flow`.

```
!  
interface Ethernet1/1  
 ip address 10.11.0.1 255.255.0.0  
 ip nat inside  
 ip route-cache policy  
 ip route-cache flow  
!
```

Опции, которые указывают IP-адрес какого интерфейса использовать для преобразования, а так же информация о версии NetFlow потока и адресе сервера с биллинговой системой NetUP UTM.

```
!  
ip nat inside source list 1 interface Ethernet1/0 overload  
ip flow-export version 5  
ip flow-export destination 10.1.0.5 9996  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.1.0.5  
!
```

Списки доступа. Первый список доступа (номер 1) используется для указания какую сеть необходимо преобразовывать во внешний IP-адрес при работе NAT. Второй список доступа (номер 108) используется для указания в `route-map`.

```
!  
access-list 1 permit 10.11.0.0 0.0.255.255  
access-list 108 permit ip any 10.11.0.0 0.0.255.255  
!
```

Правила указывающие, что если пакет направляется в сеть, указанную в списке доступа 108 (в данном случае 10.11.0.0), следует перенаправлять на интерфейс Loopback 0. Таким образом, все пакеты с внешних IP-адресов (в частности с IP-адреса 195.161.112.6) после обратного преобразования по технологии NAT попадут на интерфейс Loopback 0, где будут зафиксированы и информации о них появится в потоке NetFlow.

```
!  
route-map MAP permit 10  
 match ip address 108  
 set interface Loopback0 Ethernet1/1  
!  
End
```

В случае если информация о трафике, переданном в сторону клиента, не появляется в Netflow, проверьте:

1. Работает ли `route-map`. Для этого выполните на маршрутизаторе команду:

```
show route-map MAP
```

при этом счетчики переданных пакетов и байт должны увеличиваться.

2. Появляются ли пакеты в кэше Netflow. Для этого сразу после получения клиентом информации из Интернета выполните на маршрутизаторе команду:

```
show ip cache flow | include 195.161.112.6
```

при этом должна появиться информация о трафике примерно следующего вида:

```
Router#show ip cache flow | include 10.1.2.2
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Et1/0	195.161.112.6	Et1/1	10.11.0.6	06	0050	1093	3
Et1/1	10.11.0.6	Et1/0	195.161.112.6	06	1093	0050	5
Et1/0	195.161.112.6	Local	10.1.0.1	06	0050	1093	2

Где SrcIf – интерфейс, с которого пришел пакет. DstIf – интерфейс, на который был направлен пакет. Если данно поле Null, то данная информация не будет экспортирована в Netflow. Проверьте списки доступа.

© Компания NetUP, 2001-2005.

г.Москва, Лужнецкая набережная, д.2/4, строение 1, 5 этаж, офис 1

Почтовый адрес: 119311, Москва, а/я 87

Телефоны: +7 (095) 543-9220 (многоканальный)

+7 (095) 540-9652

+7 (095) 540-9653

