

Получение статистики с Cisco-устройств

ИКС поддерживает сборку статистики по ip-трафику с маршрутизаторов Cisco Systems по протоколу netflow версий 5 и 9.

В нашем случае ИКС находится во внутренней сети предприятия, и имеет один сетевой интерфейс. В приведенном примере использованы следующие параметры сети: Локальная сеть предприятия имеет адресацию: 192.168.0.0/255.255.255.0 Маршрутизатор Cisco – шлюз по умолчанию в сети, адрес внутреннего интерфейса: 192.168.0.254 ИКС – находится внутри локальной сети, адрес: 192.168.0.253



Настройка маршрутизатора Cisco

На маршрутизаторе мы настроим два сетевых интерфейса:

```
Ethernet1/0 с адресом 64.233.167.99/255.255.255.255  
Ethernet1/1 с адресом 192.168.0.254/255.255.255.0
```

Конфигурационный файл маршрутизатора:

```
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
!
```

Особенностью маршрутизаторов cisco является то, что маршрутизатор по netflow статистику только входящих в интерфейс пакетов. Таким образом, при использовании NAT в качестве адреса назначения для всех пакетов с внешнего интерфейса будет указан 64.233.167.99 – внешний адрес маршрутизатора. Чтобы обойти это ограничение, нам необходимо после выполнения преобразования NAT перенаправить входящий трафик ещё на какой-то интерфейс. В нашем случае используется Loopback0:

```
!
interface Loopback0
ip address 10.0.0.1 255.255.255.0
ip route-cache policy
ip route-cache flow
!
```

Для внешнего сетевого интерфейса включается NAT, экспорт netflow и указывается опция перенаправления пакетов на Loopback0:

```
!
interface Ethernet1/0
ip address 64.233.167.99 255.255.255.255
ip nat outside
ip route-cache policy
ip route-cache flow
ip policy route-map MAP
!
```

Для внутреннего сетевого интерфейса включается NAT и экспорт netflow:

```
!
interface Ethernet1/1
ip address 192.168.0.254 255.255.255.0
ip nat inside
ip route-cache policy
ip route-cache flow
!
```

Затем указываются параметры nat и адрес ИКС для экспорта netflow-статистики. Также указывается шлюз по умолчанию для доступа в интернет:

```
!
ip nat inside source list 1 interface Ethernet1/0 overload
ip flow-export version 5
ip flow-export destination 192.168.0.253 9995 (порт приема статистики на ИКС)
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 213.187.105.999
!
```

Списки доступа для nat и перенаправления трафика на Loopback0:

```
!
access-list 1 permit 192.168.0.0 0.0.0.255
access-list 108 permit ip any 192.168.0.0 0.0.0.255
!
```

Включаем SNMP сервер, чтобы мы могли получить конфигурацию сетевых интерфейсов на ИКС:

```
!
snmp-server community public R0
snmp-server ifindex persist
snmp-server enable traps tty
!
```

Правила для перенаправления трафика для списка доступа 108 в интерфейс Loopback0:

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

Более подробную информацию по настройке netflow на маршрутизаторе cisco с использованием NAT можно найти здесь: http://www.opennet.ru/base/cisco/netflow_nat.txt.html

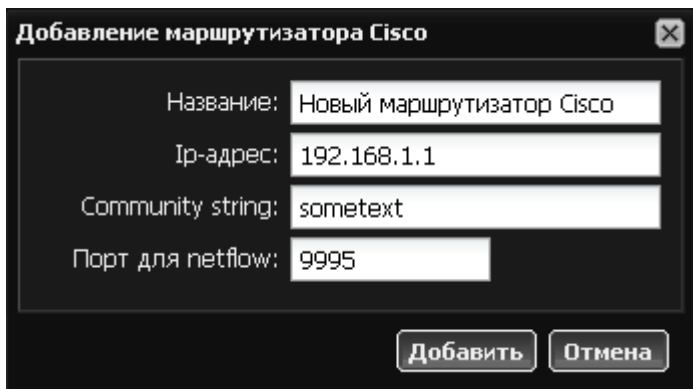
Начиная с IOS 12.3(11)T при настройке экспорта netflow, использовать loopback нет необходимости. Достаточно в настройках интерфейсов указать:

```
ip flow ingress
```

Настройка ИКС

Предполагается, что первоначальная настройка ИКС уже выполнена и локальный сетевой интерфейс сконфигурирован.

Откройте модуль «Провайдеры и сети», перейдите во вкладку «Внешние устройства». Нажмите «Добавить» → «Маршрутизатор Cisco».



Добавление маршрутизатора Cisco

Название: Новый маршрутизатор Cisco

Ip-адрес: 192.168.1.1

Community string: sometext

Порт для netflow: 9995

Добавить Отмена

В окне добавления устройство необходимо указать ip-адрес маршрутизатора. Поле Community string позволяет внести дополнительную текстовую информацию для SNMP. В поле «Порт для Netflow» указывается порт, который вы предварительно прописали в конфигурации cisco-устройства.

Теперь вы можете заводить пользователей на ИКС и выделять им адреса из локальной сети. Вся ip-статистика будет пересылаться с маршрутизатора Cisco и обрабатываться ИКС.

Важно: для того, чтобы ИКС принимал netflow-статистику, необходимо, чтобы в списке пользователей был создан пользователь с присвоенным ему ip-адресом Cisco-маршрутизатора!

Следует заметить, что если ИКС не используется в качестве интернет-шлюза организации, то он не сможет выполнять функции контроля доступа клиентов в интернет, так как трафик клиентов идёт через маршрутизатор в обход ИКС.

From:
<https://doc.a-real.ru/> - Документация

Permanent link:
<https://doc.a-real.ru/doku.php?id=en:cisco>

Last update: 2020/01/27 16:28

