Настройка экспорта сетевых потоков на «С-Терра Шлюз»

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.
Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Назначение документа

Документ описывает настройку экспорта сетевых потоков при помощи протокола NetFlow v9 (либо IPFIX) на криптошлюзах «С-Терра Шлюз» версии 5.0.

Предварительные требования

Требования к квалификации администратора

Администратор должен обладать обширными знаниями в области сетевой информационной безопасности, иметь опыт работы с аналогичным оборудованием/программным обеспечением, знать и понимать следующие технологии и протоколы: IPsec, NAT, Firewall, Routing, NetFlow, IPFIX.

Требования к начальному состоянию «С-Терра Шлюз»

Устройство «С-Терра Шлюз» должно быть инициализировано (подробнее на https://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз 5.0 -> «Подключение ПАК и инициализация С-Терра Шлюз на вычислительных системах архитектуры Intel x86-64»).

© 2003-2025 S-Terra CSP

Схема стенда

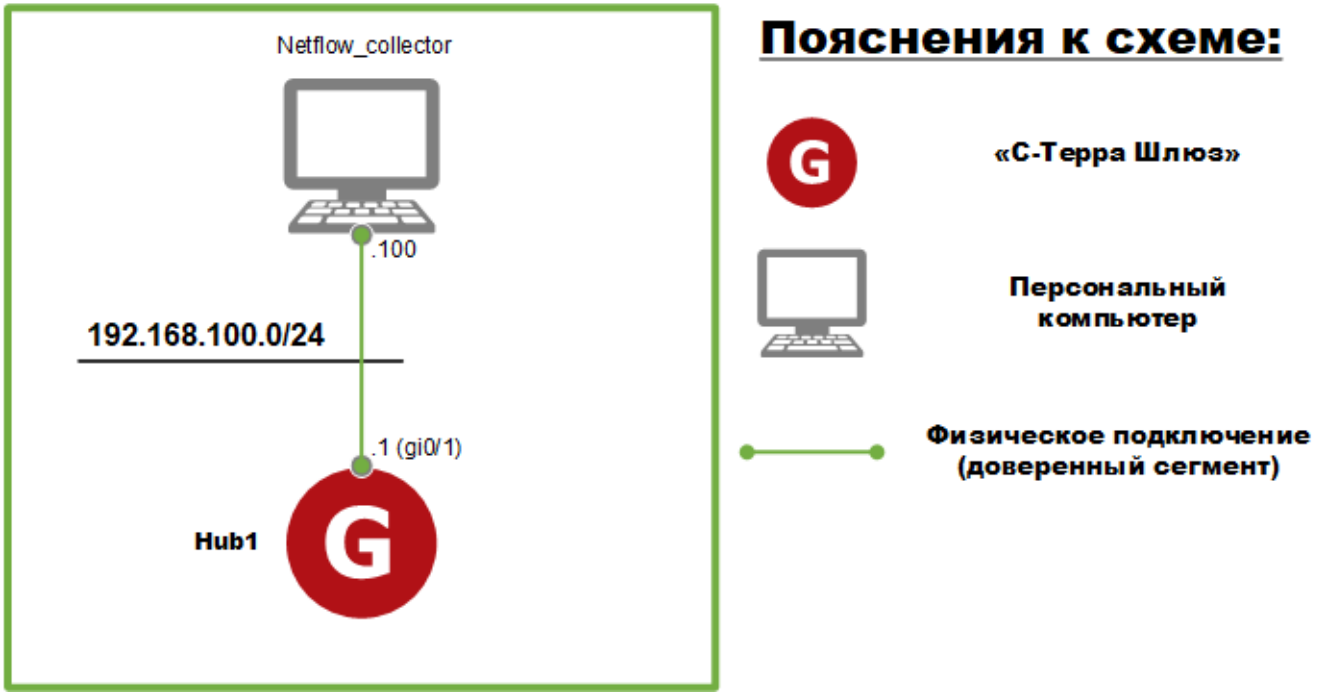


Рисунок 1. Схема взаимодействия

Ограничения и особенности

1. Выборка трафика, который нужно экспортировать на коллектор, производится при помощи утилиты `iptables`.
2. Входящий IPsec трафик не может быть экспортирован никаким образом. Исходящий IPsec трафик может быть экспортирован только в том случае, если включена повторная маршрутизация зашифрованного трафика (команда `set re-route on` в режиме настройки криптокарты в cisco-like консоли). Включение повторной маршрутизации будет приводить к снижению производительности.
3. Рекомендуется экспортировать информацию о потоках только транзитного трафика, который либо будет шифроваться, либо уже расшифрован или должен пройти в открытом виде. Для этого в `iptables`, при выборе трафика, нужно использовать цепочку `FORWARD`.

Коллектор NetFlow

В целях тестирования в качестве коллектора NetFlow можно использовать, например, Grafolean (https://github.com/grafolean/grafolean).

Настройка NetFlow

1. Войдите в CLI разграничения доступа. Для этого, после появления сообщения:

   ```
   S-Terra administrative console
   ```

   введите логин и пароль для CLI разграничения доступа:

Пользователь и пароль по умолчанию: `administrator`, `s-terra`. Обязательно смените пароль для пользователя `administrator` при помощи команды `change user password`.

```
login as: administrator
administrator's password:
```

```
administrator@sterragate]
```

2. Войдите в linux bash:

```
administrator@sterragate] system
```

```
Entering system shell...
```

3. Создайте и отредактируйте конфигурационный файл `/etc/modprobe.d/ipt_netflow.conf` модуля экспорта потоков (`ipt_NETFLOW`), например:

```
root@sterragate:~# vim.tiny /etc/modprobe.d/ipt_netflow.conf
```

```
options ipt_NETFLOW destination=192.168.100.100:2055@192.168.100.1 protocol=9
```

где:

- `options ipt_NETFLOW` – параметр указывает, что настойки будут применяться к модулю ядра `ipt_NETFLOW`
- `destination=192.168.100.100:2055@192.168.100.1` – параметр задает настройки подключения к коллектору в формате `collector_ip:collector_port@local_src_ip`. То есть `destination=192.168.100.100:2055@192.168.100.1` задает экспорт потоков на коллектор с IP адресом 192.168.100.100 и UDP-портом 2055, а в качестве IP адреса источника для пакетов будет использован IP адрес 192.168.100.1.
- `protocol=9` – параметр задает протокол экспорта потоков, 9 – NetFlow v9, 10 - IPFIX.

Подробности по настройке можно посмотреть на https://github.com/aabc/ipt-netflow

4. При помощи утилиты `iptables` выберите трафик, информацию о потоках которого нужно экспортировать на коллектор для анализа. Например, для экспорта всего транзитного трафика:

```
root@sterragate:~# iptables -I FORWARD -j NETFLOW
```

Для указания конкретного трафика можно использовать стандартные фильтры в `iptables`, например:

```
root@sterragate:~# iptables -I FORWARD -s 192.168.100.0/24 -d 192.168.1.0/24 -j NETFLOW
```

Действие -j NETFLOW указывается для всех версий протокола NetFlow и IPFIX.

5. Сохраните правила `iptables` (правила сохраняются в файл `/etc/iptables/rules.v4`):

```
root@sterragate:~# netfilter-persistent save
```

```
run-parts: executing /usr/share/netfilter-persistent/plugins.d/10-ipset save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/40-ipset save
```

6. Для просмотра текущих правил iptables используйте команду:

```
root@sterragate:~# iptables -L -n -v
```

```
Chain INPUT (policy ACCEPT 1007 packets, 140K bytes)
 pkts bytes target   prot opt in   out   source        destination

Chain FORWARD (policy ACCEPT 654 packets, 783K bytes)
```

```
 pkts bytes target   prot opt in   out   source        destination
 56   68768 NETFLOW  all  --  *    *     0.0.0.0/0     0.0.0.0/0      NETFLOW

Chain OUTPUT (policy ACCEPT 233 packets, 23308 bytes)
 pkts bytes target   prot opt in   out   source        destination
```

Изменение настроек Netflow

Если требуется изменить параметры в конфигурационном файле `/etc/modprobe.d/ipt_netflow.conf`, выполните следующие действия:

1. При помощи утилиты `iptables` удалите все правила с действием NETFLOW, например:

   ```
   root@sterragate:~# iptables -D FORWARD -j NETFLOW
   ```

2. Отредактируйте конфигурационный файл `/etc/modprobe.d/ipt_netflow.conf`.

3. Выгрузите, а затем снова загрузите модуль `ipt_NETFLOW`:

   ```
   root@sterragate:~# modprobe -r -f ipt_NETFLOW
   root@sterragate:~# modprobe ipt_NETFLOW
   ```

4. Восстановите правила `iptables` с действием NETFLOW.

Просмотр информации Netflow

Общая информация и статистика находятся в файле `/proc/net/stat/ipt_netflow`:

```
ipt_NETFLOW 2.5.1, srcversion 990F9C6B7EB3DEEA997317B; dir mac nel promisc+mpls samp
snmp vlan
Protocol version 9 (netflow), refresh-rate 20, timeout-rate 30, (templates 8, active
8).
Timeouts: active 1800s, inactive 15s. Maxflows 2000000
Flow sampling is disabled.
Promisc hack is disabled (observed 0 packets, discarded 0).
Natevents disabled, count start 0, stop 0.
Flows: active 18 (peak 21 reached 1d1h51m ago), mem 964K, worker delay 25/250 [1..25]
(0 ms, 0 us, 18:0 [cpu0]).
Hash: size 122989 (mem 960K), metric 1.00 [1.00, 1.00, 1.00]. InHash: 113 pkt, 148 K,
InPDU 21, 18996.
Rate: 23036 bits/sec, 2 packets/sec; Avg 1 min: 23337 bps, 0 pps; 5 min: 23425 bps, 0
pps
cpu#     pps; <search found new [metric], trunc frag alloc maxflows>, traffic: <pkt,
bytes>, drop: <pkt, bytes>
Total      2;      0   9501   8474 [1.00],    0    0    0    0, traffic: 17975, 18
MB, drop: 0, 0 K
cpu0       0;      0     90    385 [1.00],    0    0    0    0, traffic: 475, 0 MB,
drop: 0, 0 K
cpu1       2;      0   9121   3531 [1.00],    0    0    0    0, traffic: 12652, 12
MB, drop: 0, 0 K
cpu2       0;      0    100   2260 [1.00],    0    0    0    0, traffic: 2360, 3 MB,
drop: 0, 0 K
cpu3       0;      0    190   2298 [1.00],    0    0    0    0, traffic: 2488, 3 MB,
drop: 0, 0 K
Export: Rate 0 bytes/s; Total 2306 pkts, 0 MB, 8441 flows; Errors 0 pkts; Traffic
lost 0 pkts, 0 Kbytes, 0 flows.
sock0: 192.168.100.100:2055@192.168.100.1, sndbuf 229376, filled 1, peak 3841; err:
sndbuf reached 0, connect 0, cberr 0, other 0
```

Информация о сетевых потоках находится в файле `/proc/net/stat/ipt_netflow_flows`:

```
# hash a dev:i,o snmp:i,o mac:src,dst vlan type proto src:ip,port dst:ip,port nexthop
tos,tcpflags,options,tcpoptions packets bytes ts:first,last
1  1d50a  0  2,3  2,3  5f:ab:7a:8f:e2:91,b9:e6:00:00:09:1b  0800  1  192.168.1.100,0
192.168.100.100,0 0.0.0.0 0,0,0,0 1 1420 1201,1201
2  fd14  0  2,3  2,3  5f:ab:7a:8f:e2:91,b9:e6:00:00:09:19  0800  1  192.168.1.100,0
192.168.100.100,0 0.0.0.0 0,0,0,0 1 1420 1702,1702
3  9519  0  3,2  3,2  00:50:56:9e:92:5b,00:50:56:9e:d9:aa  0800  1  192.168.100.100,0
192.168.1.100,2048 172.16.100.1 0,0,0,0 445 631900 111362,200
```