

NetFlow

Wi-Fi , , WNAM NetFlow, /.

, "" , (NAT). , " vk.com" , , .

(Mikrotik, Cisco-) () , IP- . , , .

! NetFlow (URL) . , SSL () (DPI).

1.2 1.5.2222 WNAM () NetFlow MongoDB . :

- - NetFlow;
- , ;
- .

:

- , (MongoDB);
- NetFlow .

1.5.2222 WNAM NetFlow, :

- NetFlow - nfcapd, ;
- WNAM nfcap .

NetFlow flows, , . / NetFlow , . . , NetFlow.

WNAM 1.5.2222 Netflow UDP- 20002. /home/wnam/wnam.properties :

```
is_netflow_internal=false
```

nfdump :

```
apt-get install nfdump
```

, . , UDP- , ...:

```
vi /etc/default/nfdump
nfcapd_start=yes
```

:

```
service nfdump restart
```

:

```
service nfdump status
```

:

```
nfdump.service - netflow capture daemon
Loaded: loaded (/lib/systemd/system/nfdump.service; enabled; vendor preset:
enabled)
Active: inactive (dead) since Fri 2019-08-09 13:51:13 MSK; 3s ago
Process: 15298 ExecStart=/usr/bin/nfcapd -D -l /var/cache/nfdump -P /var/run
/nfcapd.pid -p 2055 (code=exited, status=0/SUCCESS)
Main PID: 15298 (code=exited, status=0/SUCCESS)
Tasks: 1 (limit: 4915)
CGroup: /system.slice/nfdump.service
15300 /usr/bin/nfcapd -D -l /var/cache/nfdump -P /var/run/nfcapd.pid -p 2055

09 13:51:13 debian64 systemd[1]: Started netflow capture daemon.
09 13:51:13 debian64 nfcapd[15300]: Startup.
09 13:51:13 debian64 nfcapd[15300]: Init IPFIX: Max number of IPFIX tags: 62
```

netflow- /var/cache/nfdump. .

```
root@debian64:~# ls -lat /var/cache/nfdump/ | head -n 20

drwxr-xr-x 2 root root 1523712  9 13:51 .
-rw-r--r-- 1 root root 276  9 13:51 nfcapd.current.15298
-rw-r--r-- 1 root root 9948  9 13:51 nfcapd.201908091347
-rw-r--r-- 1 root root 18740  9 13:47 nfcapd.201908091342
-rw-r--r-- 1 root root 14260  9 13:42 nfcapd.201908091337
-rw-r--r-- 1 root root 18236  9 13:37 nfcapd.201908091332
-rw-r--r-- 1 root root 15492  9 13:32 nfcapd.201908091327
```

/home/wnam/wnam.properties (java- wnam), , . :

```
nfdump_path=          nfdump,      /usr/bin/nfdump
nfdump_db=            ,      /var/cache/nfdump
```



NetFlow . WNAM 1.

/

Mikrotik.



, , (NAT) IP- .

CAPsMAN

Wireless

Interfaces

Bridge

Switch

PPP

Mesh

IP

ARP

Accounting

Addresses

Cloud

DHCP Client

DHCP Relay

DHCP Server

DNS

Firewall

Hotspot

IPsec

Kid Control

Neighbors

Packing

Pool

Routes

SMB

SNMP

Services

Settings

Socks

TFTP

Traffic Flow

RouterOS v6.45.2 (stable)

Apply

Targets

Enabled

☒

Interfaces

bridge

Cache Entries

16k

Active Flow Timeout

00:03:00

Inactive Flow Timeout

00:00:15

Last Forwarded

☒

Packets

☒

In Interface

☒

Src. Address

☒

Src. Port

☒

Protocol

☒

Gateway

☒

Dst. Address Mask

☒

Dst. MAC Address

☒

- , "- ".

WNAM (nfcapd 2055).

CAPsMAN

Wireless

Interfaces

Bridge

Switch

PPP

Mesh

IP

ARP

Accounting

Addresses

Cloud

DHCP Client

DHCP Relay

DHCP Server

DNS

Firewall

RouterOS v6.45.2 (stable)

OK

Cancel

Apply

Remove

Enabled

☒

Src. Address

Dst. Address

172.16.130.13

Port

2055

Version

5

v9/IPFIX Template Refresh

20

v9/IPFIX Template Timeout

1800

IP-, NetFlow, iptables WNAM.

!

IP- , (NetFlow).

WNAM "" , "" , "" . "" "" "" NetFlow". (), IP- , Wi-Fi (), () .

Поиск по базе данных NetFlow

- Все площадки -

- Выбрать диапазон дат -

08.08.2019 13:04:51

09.08.2019 15:04:51

Сформировать

Укажите IP адрес посещенного ресурса или ссылку на него (URL):

vk.com

15

:

04

:

51

"" (nfdump), WNAM . .

Поиск по базе данных NetFlow

- Все площадки -

Последние сутки

Сформировать

Укажите IP адрес посещенного ресурса или ссылку на него (URL):

Все IP адреса, соответствующие ссылке
23.105.225.229

Данные из таблицы "потоки" (16)

Время	URL	Число байт
08.08.2019 23:29:36 - 08.08.2019 23:29:36	TCP 10.130.129.91:56017 -> 23.105.225.229:443	4559
08.08.2019 23:29:36 - 08.08.2019 23:29:36	TCP 23.105.225.229:443 -> 10.130.129.91:56017	81948
08.08.2019 23:29:36 - 08.08.2019 23:29:36	TCP 10.130.129.91:56018 -> 23.105.225.229:443	2851
08.08.2019 23:29:36 - 08.08.2019 23:29:36	TCP 23.105.225.229:443 -> 10.130.129.91:56018	47097
08.08.2019 23:29:37 - 08.08.2019 23:29:37	TCP 10.130.129.91:56045 -> 23.105.225.229:443	2054
08.08.2019 23:29:37 - 08.08.2019 23:29:37	TCP 23.105.225.229:443 -> 10.130.129.91:56045	6573
08.08.2019 23:29:37 - 08.08.2019 23:29:37	TCP 10.130.129.91:56048 -> 23.105.225.229:443	2265
08.08.2019 23:29:37 - 08.08.2019 23:29:37	TCP 23.105.225.229:443 -> 10.130.129.91:56048	11174
08.08.2019 23:30:07 - 08.08.2019 23:30:07	TCP 10.130.129.91:56017 -> 23.105.225.229:443	187
08.08.2019 23:30:07 - 08.08.2019 23:30:07	TCP 10.130.129.91:56018 -> 23.105.225.229:443	187
08.08.2019 23:30:07 - 08.08.2019 23:30:07	TCP 23.105.225.229:443 -> 10.130.129.91:56017	104
08.08.2019 23:30:07 - 08.08.2019 23:30:07	TCP 23.105.225.229:443 -> 10.130.129.91:56018	104
08.08.2019 23:30:08 - 08.08.2019 23:30:08	TCP 10.130.129.91:56048 -> 23.105.225.229:443	187
08.08.2019 23:30:08 - 08.08.2019 23:30:08	TCP 23.105.225.229:443 -> 10.130.129.91:56048	52
08.08.2019 23:30:08 - 08.08.2019 23:30:08	TCP 10.130.129.91:56045 -> 23.105.225.229:443	187
08.08.2019 23:30:08 - 08.08.2019 23:30:08	TCP 23.105.225.229:443 -> 10.130.129.91:56045	104

Список сессий (2)

MAC	IP	Площадка	Время	Отправлено	Передано
74:9E:AF:6C:3F:20	10.130.129.91	WNAM_TEST_129	08.08.2019 23:24:31 +2 мин.	2660	17486
74:9E:AF:6C:3F:20	10.130.129.91	WNAM_TEST_129	08.08.2019 23:28:56 +6 мин.	49055	49726

Список пользователей (1)

MAC	Телефон	DHCP-идентификатор	Число сессий
74:9E:AF:6C:3F:20	79999662211		2

Выгрузить в файл

" IP- (URL)" IP-, . DNS-, IP- (IP) DNS WNAM .



, (Wi-Fi). " " - . - 1000 . , .
(rep_search_nf.csv) (Excel). ().

1	Период	08.08.2019 13:04	09.08.2019 15:04		
2	URL	vk.com			
3	Данные из таблицы "потоки"				
4	Время	URL	Число байт		
5	08.08.2019 23:29:43 - 08.08.2019 23:29:43	TCP 10.130.129.91:56088 -> 93.186.225.197:80	581		
6	08.08.2019 23:29:43 - 08.08.2019 23:29:43	TCP 93.186.225.197:80 -> 10.130.129.91:56088	587		
7	08.08.2019 23:29:43 - 08.08.2019 23:29:43	TCP 10.130.129.91:56089 -> 93.186.225.197:443	1852		
8	08.08.2019 23:29:43 - 08.08.2019 23:29:43	TCP 93.186.225.197:443 -> 10.130.129.91:56089	5862		
9	08.08.2019 23:30:12 - 08.08.2019 23:30:12	TCP 10.130.129.91:56088 -> 93.186.225.197:80	40		
10	08.08.2019 23:30:12 - 08.08.2019 23:30:12	TCP 10.130.129.91:56089 -> 93.186.225.197:443	40		
11					
12	Список сессий				
13	MAC	IP	Площадка	Время	Отправлено Передано
14	74:9E:AF:6C:3F:20	10.130.129.91	WNAM_TEST_129	08.08.2019 23:24:31 +2 мин.	2660 17486
15	74:9E:AF:6C:3F:20	10.130.129.91	WNAM_TEST_129	08.08.2019 23:28:56 +6 мин.	49055 49726
16					
17	Список пользователей				
18	MAC	Телефон	DHCP-идентификатор	Число сессий	
19	74:9E:AF:6C:3F:20	79999662211		2	

Потоки сессии 80a00011-190808-6c3f20

Пользователь: 10.130.129.91 [74:9E:AF:6C:3F:20] , площадка: 101 WNAM_TEST_129

Показывать: 10 записей на странице

URL	Время	Пакетов	Байт
TCP 88.212.252.22:443 -> 10.130.129.91:56034	08.08.2019 23:30:08	0	239
TCP 10.130.129.91:56041 -> 80.239.201.31:443	08.08.2019 23:30:08	0	187
TCP 10.130.129.91:56044 -> 80.239.201.31:443	08.08.2019 23:30:08	0	187
TCP 10.130.129.91:56045 -> 23.105.225.229:443	08.08.2019 23:30:08	0	187
TCP 23.105.225.229:443 -> 10.130.129.91:56045	08.08.2019 23:30:08	0	104
TCP 80.239.201.31:443 -> 10.130.129.91:56041	08.08.2019 23:30:08	0	104
TCP 80.239.201.31:443 -> 10.130.129.91:56044	08.08.2019 23:30:08	0	104
TCP 10.130.129.91:56070 -> 87.250.250.119:443	08.08.2019 23:30:10	0	187
TCP 10.130.129.91:56071 -> 87.250.250.119:443	08.08.2019 23:30:10	0	187
TCP 10.130.129.91:56078 -> 213.180.204.158:443	08.08.2019 23:30:10	0	187
TCP 10.130.129.91:56080 -> 213.180.204.158:443	08.08.2019 23:30:10	0	187

Показано с 301 по 310 из 406 записей

Предыдущая1...303132...41Следующая

- ;
- , NetFlow.

WNAM Zabbix. , cron ():

```
find /var/cache/nfdump -type f -ctime +90 -exec rm {} \;
```

NetFlow rsync :

```
rsync --delete -acvz -e ssh /var/cache/nfdump backup@backup-wnam.provider.ru:
nfdump
```

NetFlow (nfcapd) WNAM "" " "Netflow".

Работа с базой данных

MongoDB Очистка Commonbase Netflow

Параметры хранилища Netflow

Путь до хранилища данных

/var/cache/nfdump

Дисковый том

/dev/sda1

Объем тома, Гб

14.934494

ЗАНЯТО

12.391834

%

82

Статистика хранилища Netflow

```
Ident: none
Flows: 6316152
Flows_tcp: 3167630
Flows_udp: 3141754
Flows_icmp: 739
Flows_other: 6029
Packets: 97043305
Packets_tcp: 74267692
Packets_udp: 21677784
Packets_icmp: 2275
Packets_other: 1095554
Bytes: 69582756480
Bytes_tcp: 56811955530
Bytes_udp: 12700109742
Bytes_icmp: 576256
Bytes_other: 70114952
First: 1554064253 ( 31.03.2019 23:30:53 )
Last: 1565463345 ( 10.08.2019 21:55:45 )
msec_first: 46
msec_last: 512
Sequence failures: 1442
```