PacketController Network Monitor

Version: 7.3.8

Updated: June 2022

PacketController Network

Disclaimer

Table of Contents

Overview

PacketController provides real time traffic capture feature, which will give the ISP complete details on its network and subscribers.

The traffic capture runs continuously and keeps track of all the connections and hosts in ISP network.

Some use cases as below:

- Show top usage of connections to see bandwidth hog
- Show top usage of hosts
- Show top PPS (packet per second) hosts to see abnormal traffic like DDoS attack and identify its source IP addresses

High Performance

- PacketController Network Monitor scales at 1Gbps (full duplex)
- At 1Gbps, you could use both network monitor and bandwidth management without the performance compromise

Real time network monitoring on whole network

- Real-time traffic capture for the whole network, i.e., all the active connections on the network and top 50 talkers and hosts
- For each active connection, its source IP address, destination IP address, source port, destination port, DNS, protocol, URL (if the protocol is HTTP/HTTPs), live bandwidth usage of this connection
- Host Geo Location

Real time network monitoring per subscriber

- Real-time traffic snapshot for each active subscriber, i.e., all the active connections for each subscriber
- For each active connection, its source IP address, destination IP address, source port, destination port, DNS, protocol, URL (if the protocol is HTTP/HTTPs), live bandwidth usage of this connection

Sample Site

The examples shown here are simple illustrations of what can be done with PacketController network monitor in ISP environment.

Background

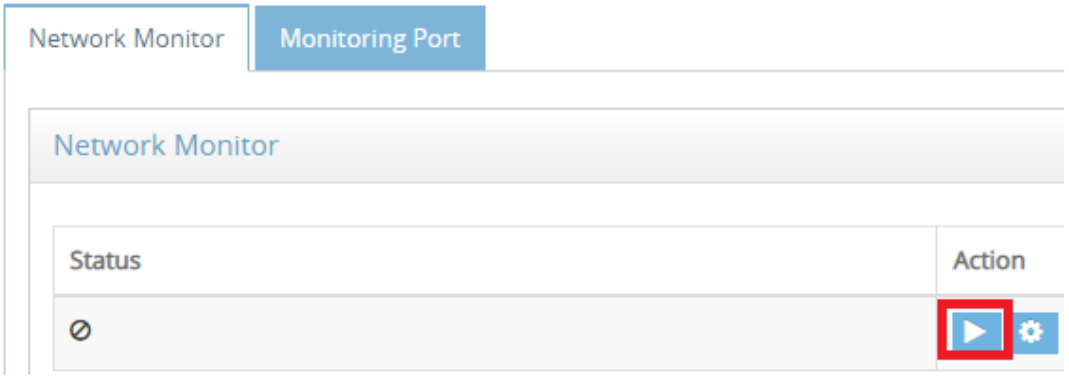
ISP A has 1000+ subscribers and the uplink is at 600Mbps.

Objective

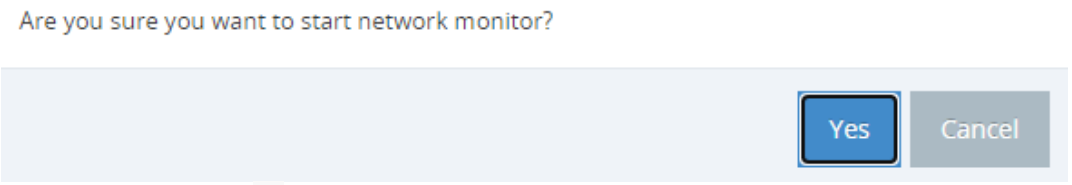
- **Network connection tracking:** ISP A needs to know the number of active connections on its network, and the real time bandwidth usage of each connection. This is good source to understand the network load; Furthermore, it is good to know if there are abnormal network activities like DDoS attacks.
- **Subscriber-based connection tracking**: Besides the live bandwidth usage for each subscriber, ISP A needs to know real time active connections for each subscriber. This is to provide connection-based stats for helpdesk people to deal with customer complaints.

Enable Network Monitor

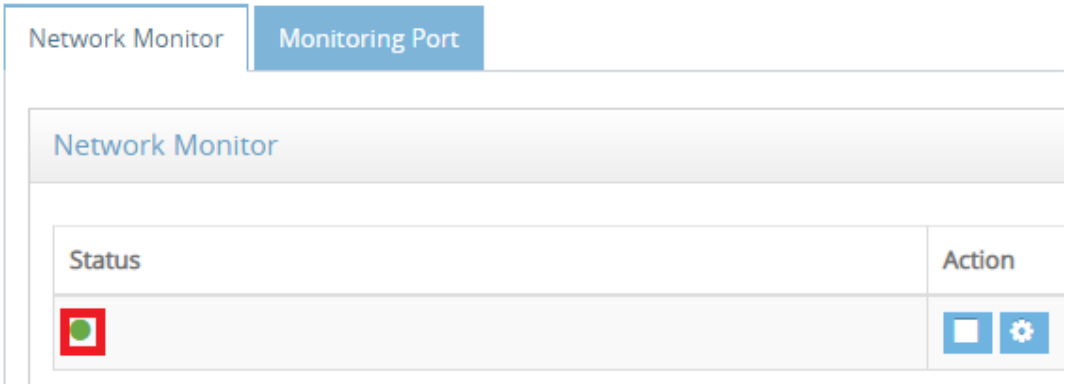
- Click Network -> Monitor, in Network Monitor tab and click  icon in Action column



- In the popup window, click **Yes** button



- In Status column, the  icon will be shown.



Network Monitor Settings

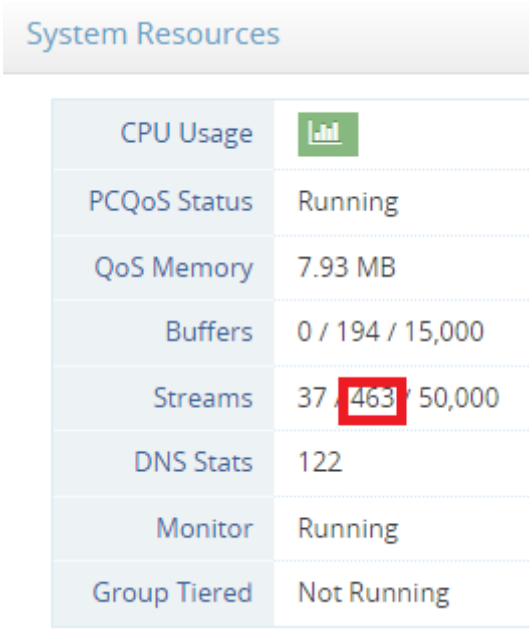
The network monitor settings can be configured, please note that the network monitor settings can ONLY be set when network monitor is not running.

In most case, the default value of network monitor settings is good to go.

So network monitor should be stopped if it is running before change the network monitor settings.

There are 2 settings:

- **Max. Connections**: The max. connections/streams to be tracked, by default it is 100,000, the valid range is 1,000 – 500,000. The max. connections/streams setting depends on network activities. You could check the current max. streams on your network in Streams of System Resource widget in Dashboard.

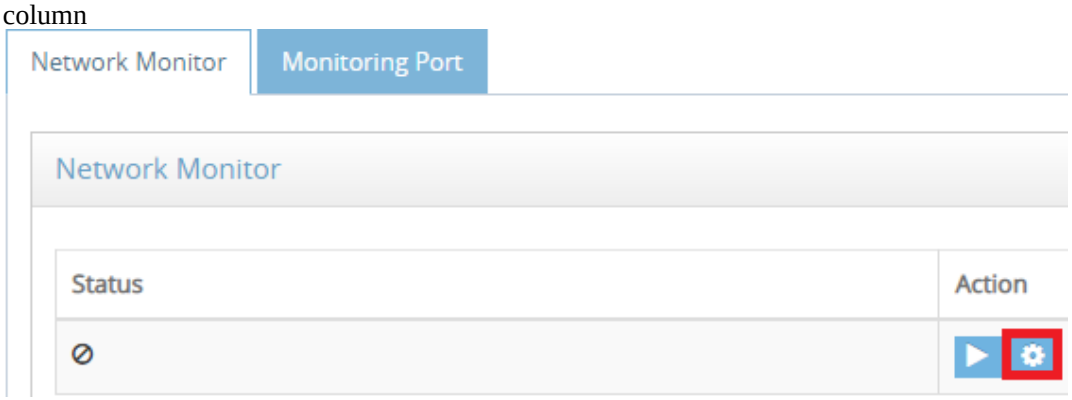


- **Max Hosts**: The max. hosts (both internal and external network) to be tracked, by default it is 25,000, the valid range is 1,000 – 50,000

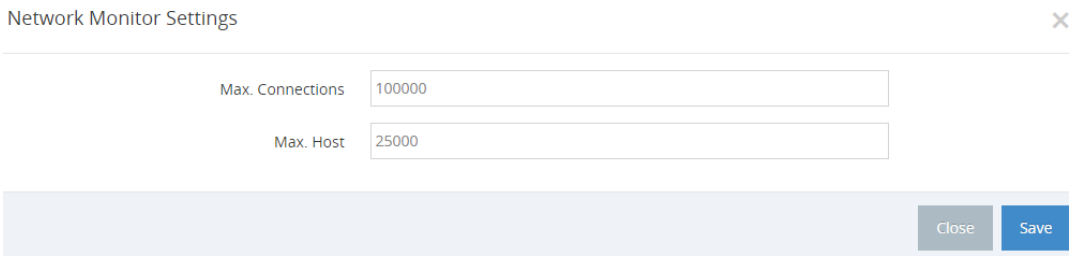
The max. connections/hosts take the resource like CPU and memory, those 2 settings should be a little more than the number of actual streams and hosts on your network.

The procedure to configure network monitor settings:

- Click Network -> Monitor, in Network Monitor tab and click  icon in Action column



- In Network Monitor Setting window, input the numbers



- Click **Save** button

Configure Monitoring Port

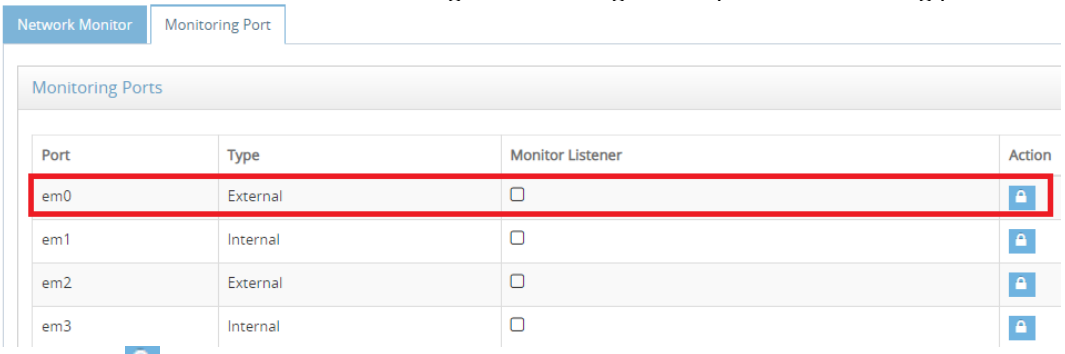
The monitoring port must be configured, it must be the external port of bridge. If you have multiple bridges and you want to monitor the traffic across all bridges, then you should

configure all external ports as monitoring ports.

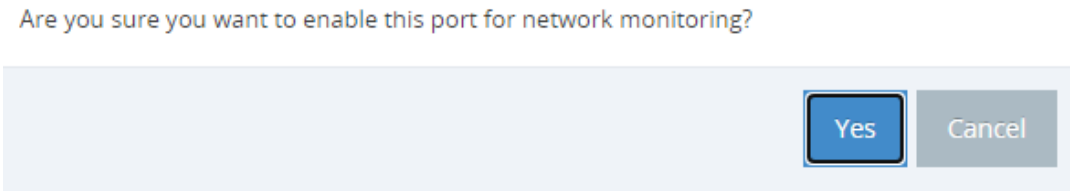
The monitoring port can be configured before or after network monitor is running.

The procedure to configure monitoring port:

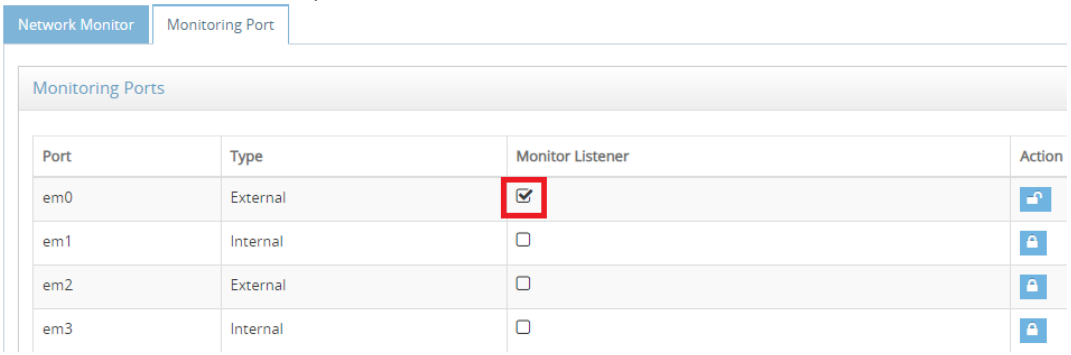
- Click Network -> Monitor, in Monitoring Port tab and go to the port for monitoring port



- Click icon  in Action column
- In the popup window, click **Yes** button



- In Monitor Listener column, the checkbox is checked.

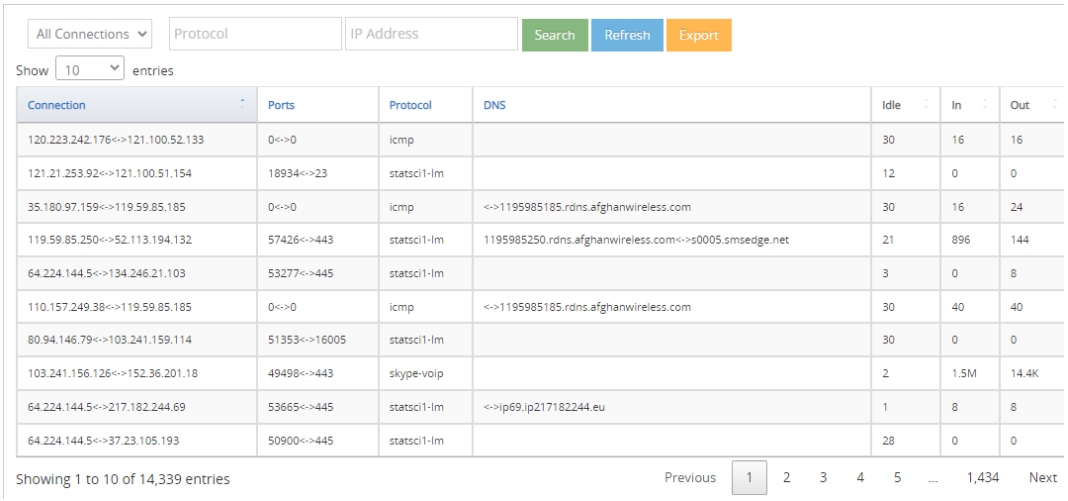


Notes:
please do NOT use internal port of bridge.

Overall Network

The active connections and hosts are monitored in real time on overall network.

- Click Log & Report -> Connections, select All connections to view all active connections



All Connections | Protocol | IP Address | Search | Refresh | Export

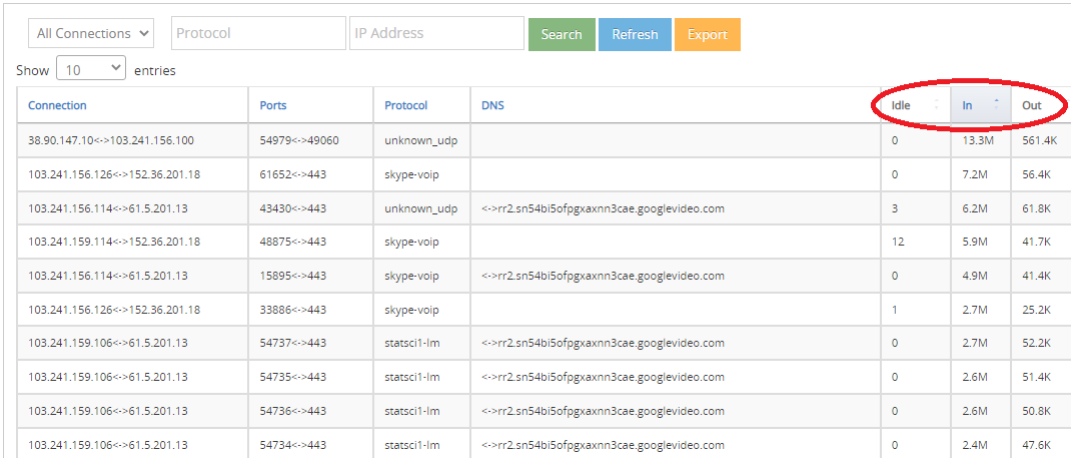
Show 10 entries

Connection	Ports	Protocol	DNS	Idle	In	Out
120.223.242.176<->121.100.52.133	0<->0	icmp		30	16	16
121.21.253.92<->121.100.51.154	18934<->23	statsci1-lm		12	0	0
35.180.97.159<->119.59.85.185	0<->0	icmp	<->1195985185.rdns.afghanwireless.com	30	16	24
119.59.85.250<->52.113.194.132	57426<->443	statsci1-lm	1195985250.rdns.afghanwireless.com<->s0005.smsedge.net	21	896	144
64.224.144.5<->134.246.21.103	53277<->445	statsci1-lm		3	0	8
110.157.249.38<->119.59.85.185	0<->0	icmp	<->1195985185.rdns.afghanwireless.com	30	40	40
80.94.146.79<->103.241.159.114	51353<->16005	statsci1-lm		30	0	0
103.241.156.126<->152.36.201.18	49498<->443	skype-voip		2	1.5M	14.4K
64.224.144.5<->217.182.244.69	53665<->445	statsci1-lm	<->ip69.ip217182244.eu	1	8	8
64.224.144.5<->37.23.105.193	50900<->445	statsci1-lm		28	0	0

Showing 1 to 10 of 14,339 entries

Previous 1 2 3 4 5 ... 1,434 Next

The column idle/In/Out can be sorted.

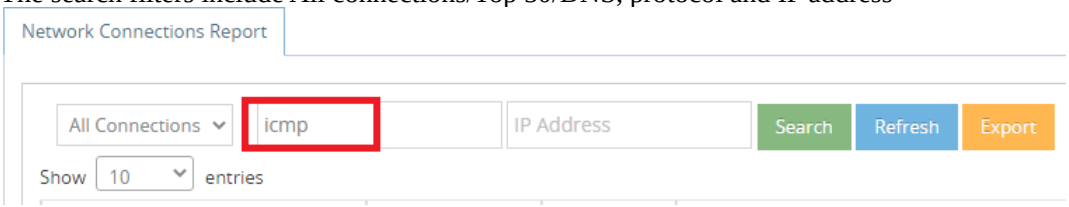


All Connections | Protocol | IP Address | Search | Refresh | Export

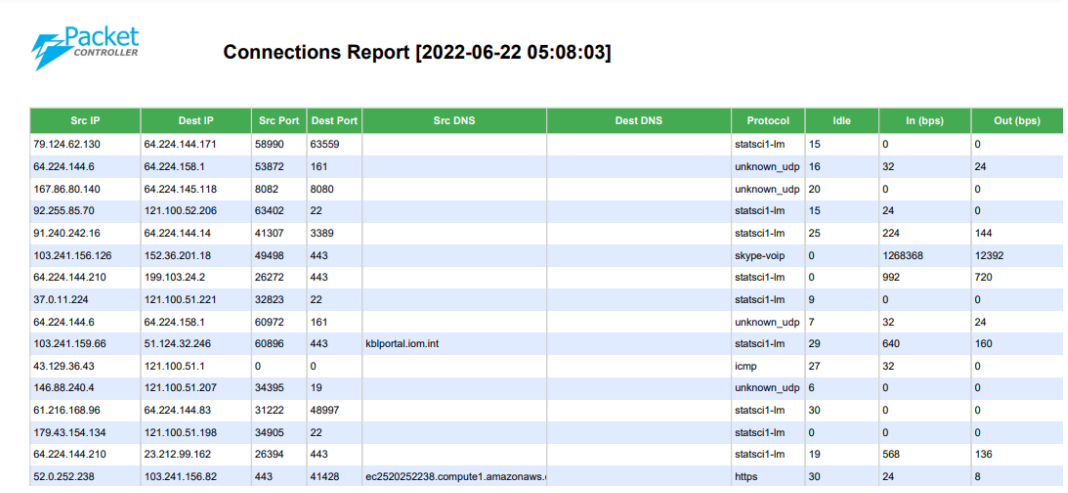
Show 10 entries

Connection	Ports	Protocol	DNS	Idle	In	Out
38.90.147.10<->103.241.156.100	54979<->49060	unknown_udp		0	13.3M	561.4K
103.241.156.126<->152.36.201.18	61652<->443	skype-voip		0	7.2M	56.4K
103.241.156.114<->61.5.201.13	43430<->443	unknown_udp	<->rr2.sn54bi5ofpgxaxnn3cae.googlevideo.com	3	6.2M	61.8K
103.241.159.114<->152.36.201.18	48875<->443	skype-voip		12	5.9M	41.7K
103.241.156.114<->61.5.201.13	15895<->443	skype-voip	<->rr2.sn54bi5ofpgxaxnn3cae.googlevideo.com	0	4.9M	41.4K
103.241.156.126<->152.36.201.18	33886<->443	skype-voip		1	2.7M	25.2K
103.241.159.106<->61.5.201.13	54737<->443	statsci1-lm	<->rr2.sn54bi5ofpgxaxnn3cae.googlevideo.com	0	2.7M	52.2K
103.241.159.106<->61.5.201.13	54735<->443	statsci1-lm	<->rr2.sn54bi5ofpgxaxnn3cae.googlevideo.com	0	2.6M	51.4K
103.241.159.106<->61.5.201.13	54736<->443	statsci1-lm	<->rr2.sn54bi5ofpgxaxnn3cae.googlevideo.com	0	2.6M	50.8K
103.241.159.106<->61.5.201.13	54734<->443	statsci1-lm	<->rr2.sn54bi5ofpgxaxnn3cae.googlevideo.com	0	2.4M	47.6K

The search filters include All connections/Top 50/DNS, protocol and IP address



All connection records can be exported in PDF.

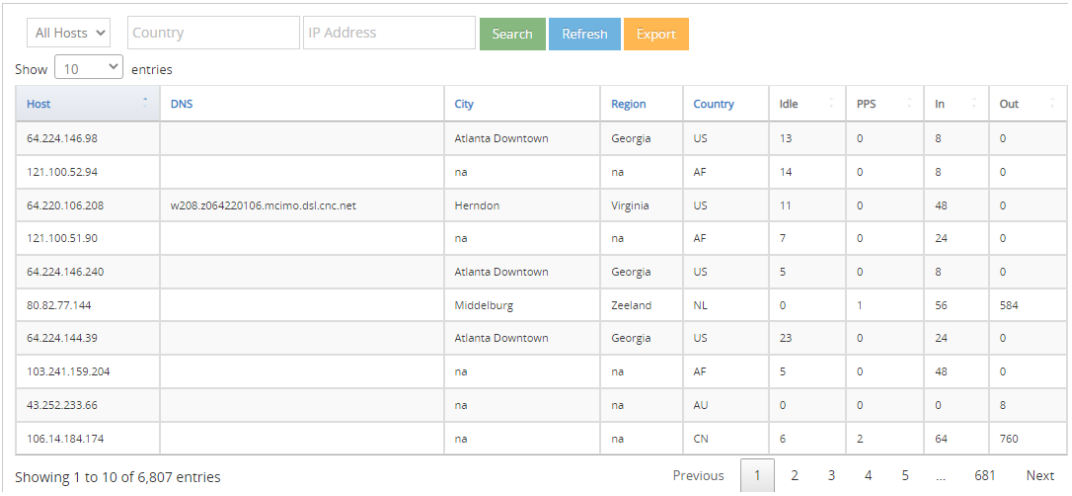


Packet CONTROLLER

Connections Report [2022-06-22 05:08:03]

Src IP	Dest IP	Src Port	Dest Port	Src DNS	Dest DNS	Protocol	Idle	In (bps)	Out (bps)
79.124.62.130	64.224.144.171	58990	63559			statsci1-lm	15	0	0
64.224.144.6	64.224.158.1	53872	161			unknown_udp	16	32	24
167.86.80.140	64.224.145.118	8082	8080			unknown_udp	20	0	0
92.255.85.70	121.100.52.206	63402	22			statsci1-lm	15	24	0
91.240.242.16	64.224.144.14	41307	3389			statsci1-lm	25	224	144
103.241.156.126	152.36.201.18	49498	443			skype-voip	0	1268368	12392
64.224.144.210	199.103.24.2	26272	443			statsci1-lm	0	992	720
37.0.11.224	121.100.51.221	32823	22			statsci1-lm	9	0	0
64.224.144.6	64.224.158.1	60972	161			unknown_udp	7	32	24
103.241.159.66	51.124.32.246	60896	443	kblportal.iom.int		statsci1-lm	29	640	160
43.129.36.43	121.100.51.1	0	0			icmp	27	32	0
146.88.240.4	121.100.51.207	34395	19			unknown_udp	6	0	0
61.216.168.96	64.224.144.83	31222	48997			statsci1-lm	30	0	0
179.43.154.134	121.100.51.198	34905	22			statsci1-lm	0	0	0
64.224.144.210	23.212.99.162	26394	443			statsci1-lm	19	568	136
52.0.252.238	103.241.156.82	443	41428	ec2520252238.compute1.amazonaws.c		https	30	24	8

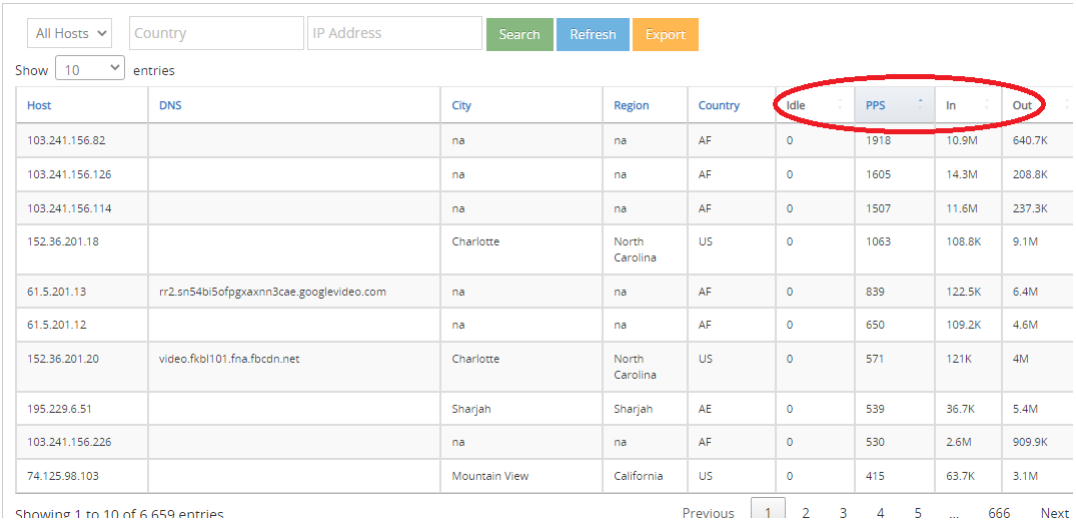
- Click Log & Report -> Host, , select All Hosts to view all active hosts including external and internal hosts



Host	DNS	City	Region	Country	Idle	PPS	In	Out
64.224.146.98		Atlanta Downtown	Georgia	US	13	0	8	0
121.100.52.94		na	na	AF	14	0	8	0
64.220.106.208	w208.z064220106.mcimo.dsl.cnc.net	Herndon	Virginia	US	11	0	48	0
121.100.51.90		na	na	AF	7	0	24	0
64.224.146.240		Atlanta Downtown	Georgia	US	5	0	8	0
80.82.77.144		Middelburg	Zeeland	NL	0	1	56	584
64.224.144.39		Atlanta Downtown	Georgia	US	23	0	24	0
103.241.159.204		na	na	AF	5	0	48	0
43.252.233.66		na	na	AU	0	0	0	8
106.14.184.174		na	na	CN	6	2	64	760

Showing 1 to 10 of 6,807 entries Previous 1 2 3 4 5 ... 681 Next

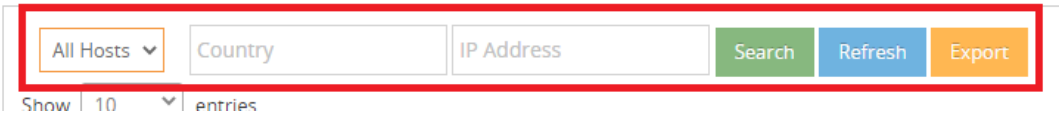
The column idle/PPS/In/Out can be sorted.



Host	DNS	City	Region	Country	Idle	PPS	In	Out
103.241.156.82		na	na	AF	0	1918	10.9M	640.7K
103.241.156.126		na	na	AF	0	1605	14.3M	208.8K
103.241.156.114		na	na	AF	0	1507	11.6M	237.3K
152.36.201.18		Charlotte	North Carolina	US	0	1063	108.8K	9.1M
61.5.201.13	rr2.sn54bi5ofpgxaxnn3cae.googlevideo.com	na	na	AF	0	839	122.5K	6.4M
61.5.201.12		na	na	AF	0	650	109.2K	4.6M
152.36.201.20	video.fkbl101.fna.fbcdn.net	Charlotte	North Carolina	US	0	571	121K	4M
195.229.6.51		Sharjah	Sharjah	AE	0	539	36.7K	5.4M
103.241.156.226		na	na	AF	0	530	2.6M	909.9K
74.125.98.103		Mountain View	California	US	0	415	63.7K	3.1M

Showing 1 to 10 of 6,659 entries Previous 1 2 3 4 5 ... 666 Next

The search filters include All Hosts/Top 50/DNS, Country and IP Address



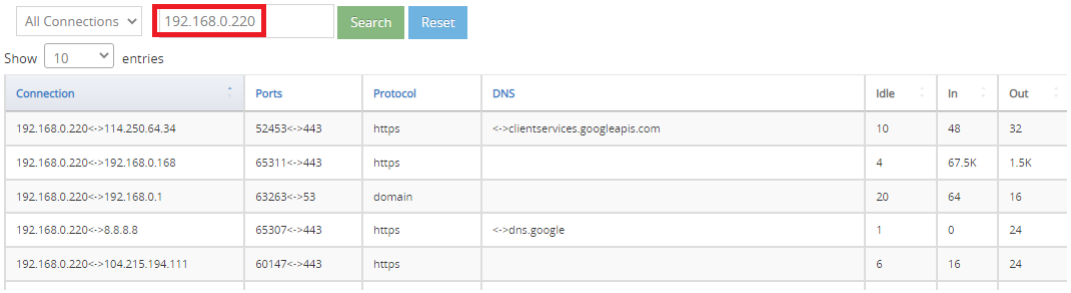
All hosts can be exported in PDF

Hosts Report [2022-06-19 12:40:01]

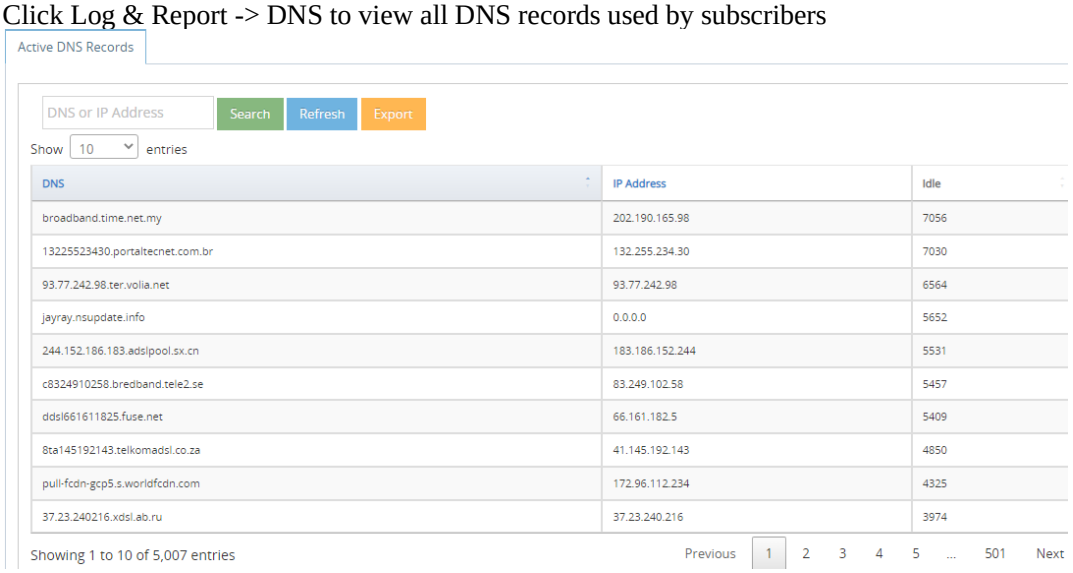
Host	DNS	City	Region	Country	Idle	PPS	In (bps)	Out (bps)
107.154.179.159	107.154.179.159.ip.incapdns.net	na	na	US	29	0	0	0
50.220.51.242		na	na	US	15	0	24	0
64.224.146.98		Atlanta Downtown	Georgia	US	8	0	16	0
121.100.52.94		na	na	AF	30	0	0	0
64.225.0.87	grippe.6228888888.uxm	na	na	US	10	0	0	32
121.100.51.90		na	na	AF	9	0	48	0
151.80.120.112		Rome	Lazio	IT	14	0	16	0
3.250.122.120		na	na	US	12	0	56	56
104.18.100.194		na	na	US	25	0	0	0
17.248.162.70		Cupertino	California	US	0	3	3448	6608
66.110.49.80		Wilmington 400	Delaware	US	14	0	128	64
64.224.144.39		Atlanta Downto	Georgia	US	11	0	56	0

Notes:

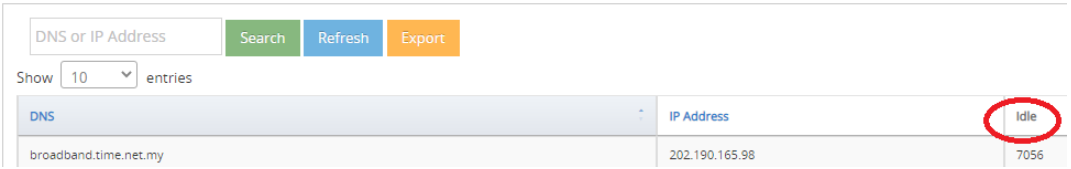
- In Host reports, PPS (Packet Per Second) metric is good to identify the DDoS attacks.
- One specific IP could be filtered for both connections and hosts in Search input.



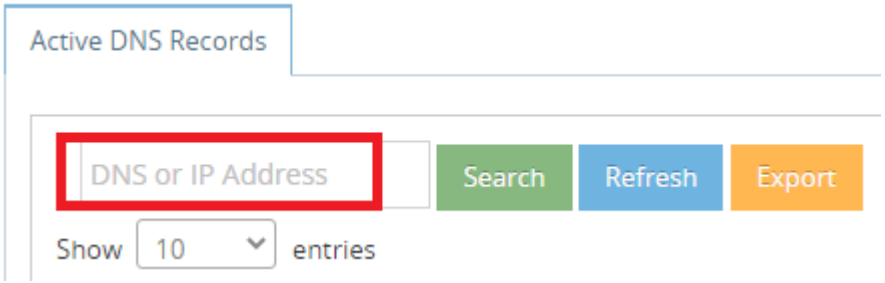
- Click Log & Report -> DNS to view all DNS records used by subscribers



The column idle can be sorted.



The search filters include DNS or IP Address



All DNS records can be exported in PDF

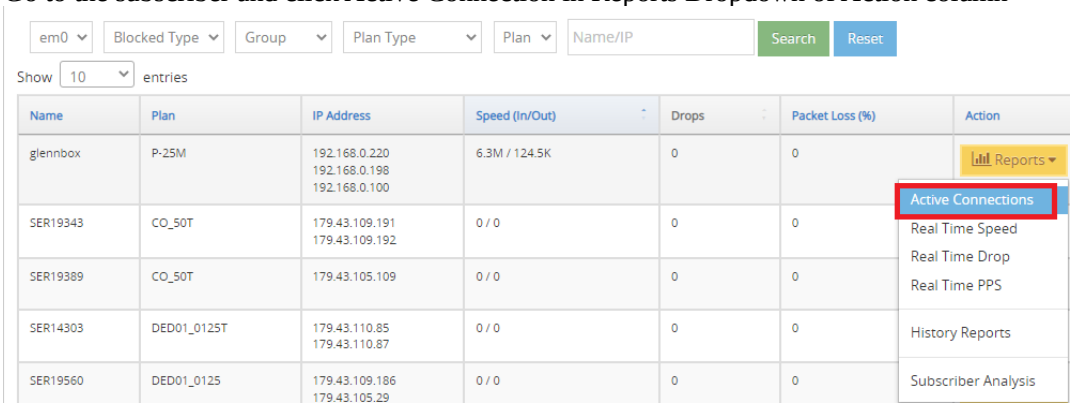
Packet CONTROLLER **Active DNS Record Report [2022-06-22 05:26:53]**

DNS	IP Address	Idle
cc38x138.sels.ru	83.172.38.138	1692
112.201.230.229.pldt.net	112.201.230.229	810
24395.endicott.edu	64.25.243.95	625
hep.tucm.site	0.0.0.0	47
c8324910258.bredband.tele2.se	83.249.102.58	14
58.69.176.162.pldt.net	58.69.176.162	1230
catv371918134.catv.fixed.vodafone.hu	37.191.8.134	1107
204.ip193702.eu	193.70.2.204	622
ip18423112582.anahca.spcsdns.net	184.231.125.82	902
sp187108200160.l3.eveocloud.net	187.108.200.160	460
177.248.89.43clienteszapizzi.mx	177.248.89.43	1465
WGPON395243.wateen.net	110.39.52.44	1046
37.23.150163.xdsl.ab.ru	37.23.150.163	989
m5936.contaboserver.net	173.212.243.136	624
WGPON3924229.wateen.net	110.39.24.229	1808
831726496.lidnet.net	83.172.64.96	1536
ehtraz.com	20.50.170.60	883
1141426228.ppp.bbiq.jp	114.142.26.228	693

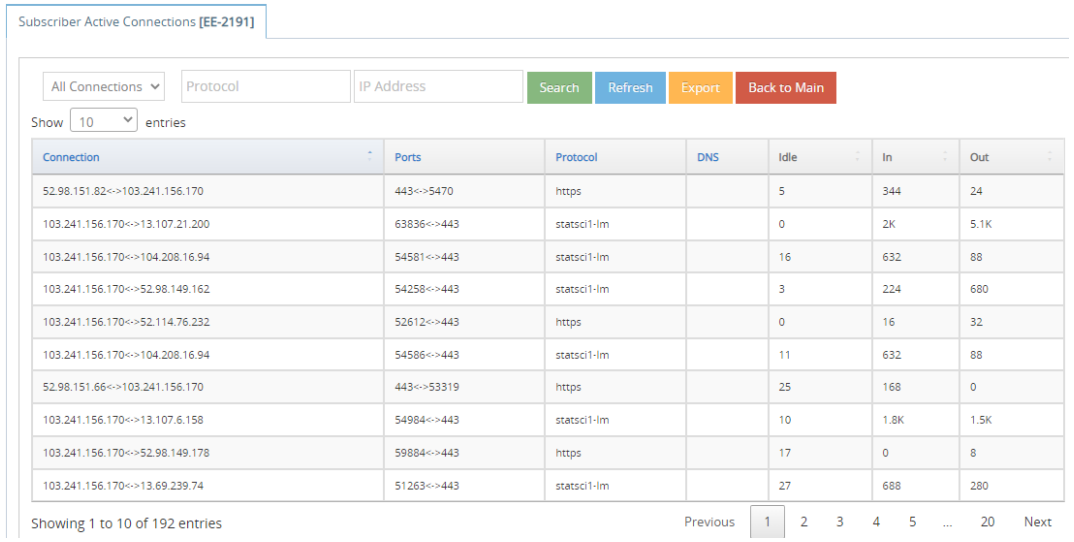
Subscriber

The active connections per subscriber are captured in real time.

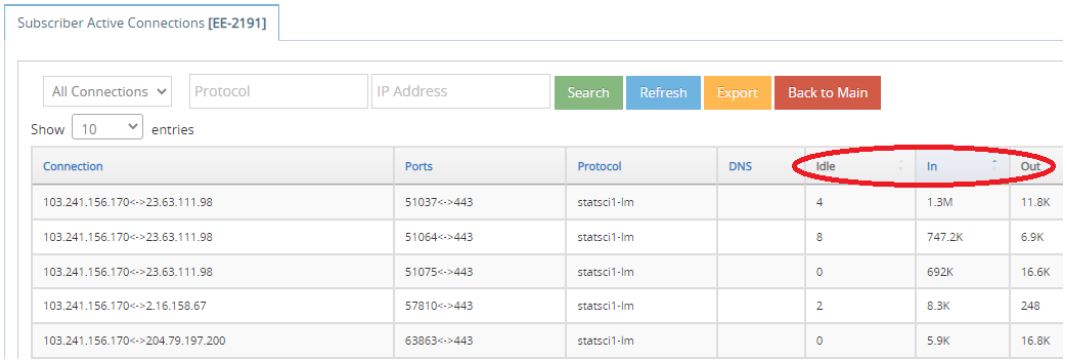
- Click Log & Report -> Subscriber
- Go to the subscriber and click Active Connection in Reports Dropdown of Action column



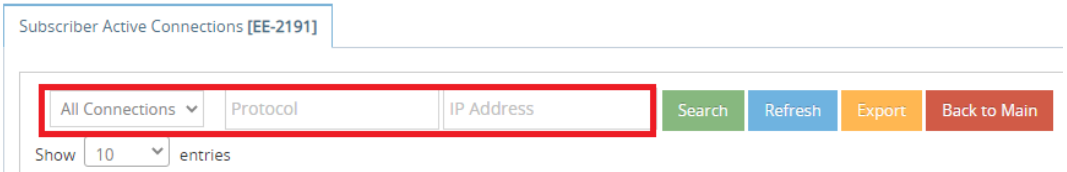
- The active connections for this subscriber shown as below:



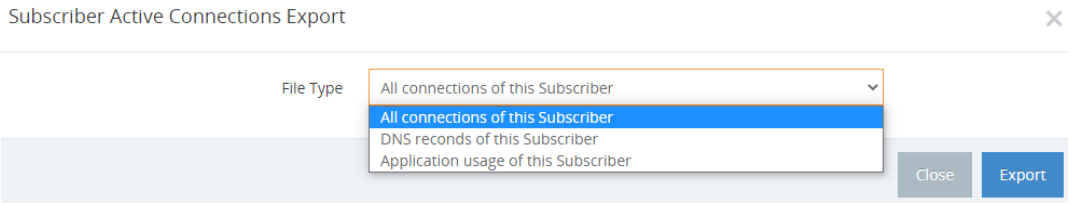
- Idle/In/Out can be sorted and it is helpful to see the heavy connections of this subscriber



- The search filters include All connections/Top 50/DNS, protocol and IP address



- There are 3 types of data which can be exported in PDF: All connections of this subscriber, DNS records of this subscriber and Application usage of this subscriber



Packet CONTROLLER

EE-2600 Connections Report [2022-06-19 12:44:41]

Src IP	Dest IP	Src Port	Dest Port	Src DNS	Dest DNS	Protocol	Idle	In	Out
103.144.237.6	61.5.201.13	61379	443		rr2.sn54bi5ofpgxaxnn3cae.googlevidec.com	skype-voip	0	5.5M	91.4K
103.144.237.182	152.36.201.20	35534	443		video.fkbl101.fna.fbcdn.net	skype-voip	0	3.1M	45.3K
179.60.195.48	103.144.237.221	3478	45730			skype-voip	0	844.4K	708.7K
103.144.237.182	152.36.201.20	55410	443		video.fkbl101.fna.fbcdn.net	unknown_udp	0	821.8K	11.1K
103.144.237.221	61.5.201.13	52166	443		rr2.sn54bi5ofpgxaxnn3cae.googlevidec.com	skype-voip	0	809.7K	20.2K
103.144.237.220	61.5.201.13	44344	443		rr2.sn54bi5ofpgxaxnn3cae.googlevidec	statsci1-lm	0	796.8K	15.4K
103.144.237.46	8.241.80.124	63077	80			bittorrent	0	761.4K	24.5K
103.144.237.222	152.36.201.18	43408	443			statsci1-lm	0	715.6K	14.6K
103.144.237.221	61.5.201.13	36448	443		rr2.sn54bi5ofpgxaxnn3cae.googlevidec.com	skype-voip	0	699.4K	26.5K
103.144.237.222	152.36.201.18	59408	443			skype-voip	0	677.7K	13.7K
103.144.237.46	61.5.201.13	58921	443		rr2.sn54bi5ofpgxaxnn3cae.googlevidec.com	unknown_udp	6	632.6K	11.6K
103.144.237.122	152.36.201.18	43921	443			unknown_udp	0	604.1K	11.1K

Packet CONTROLLER

EE-2600 DNS Report [2022-06-19 12:44:34]

DNS
httpsapihk.bigolive.tv
dns.google
240.205.226.35.bc.googleusercontent.com
tiktok.bytedance.map.fastly.net
ip.azwus1clients.msnmessenger.msn.com.akadns.net
www.google.com
msgrlatest.c10r.facebook.com
play.google.com

EE-2600 Protocol Report [2022-06-19 12:44:07]

Protocol	In	Out	Total
statsci1-lm	38.2M	1.5K	38.2M
skype-voip	27.1M	360	27.1M
unknown_udp	16.3M	0	16.3M
https	4M	1.1K	4M
p2p	2.7M	208	2.7M
msn-im	854.5K	17.7K	872.2K
kazaa	789.1K	1K	790.1K
bittorrent	750.3K	0	750.3K
unknown_tcp	225.9K	232	226.2K
domain	128.8K	24	128.8K
icmp	15.8K	32	15.8K
xmpp-client	6.4K	0	6.4K
http	6.3K	8	6.3K