Detect DDoS attacks with opFlow

Check out the original blog which inspired this page here: https://opmantek.com/network-security-determine-attack-vector-with-opflow/

Perform a quick google search for DDoS attacks and you will see that free tools used to carry out these attacks are littered all over the internet. These attacks have become increasingly easy to pull off making them a common occurrence. Identifying and preventing these attacks before they cause any damage is key in keeping your network performing smoothly. opFlow is well equipped to determine where these attacks are coming from.

The default page after opening opFlow displays the top 10 sources of network traffic. If you feel your network is under a DDoS attack, change the page to display the top 10 applications. To do this navigate to menu -> Advanced, this opens the menu below.

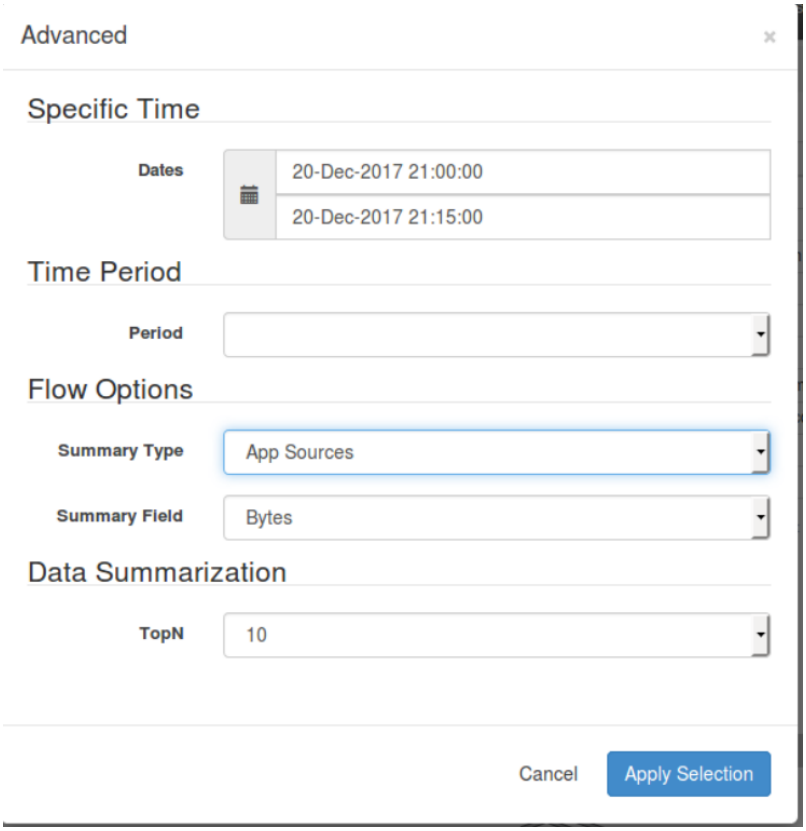
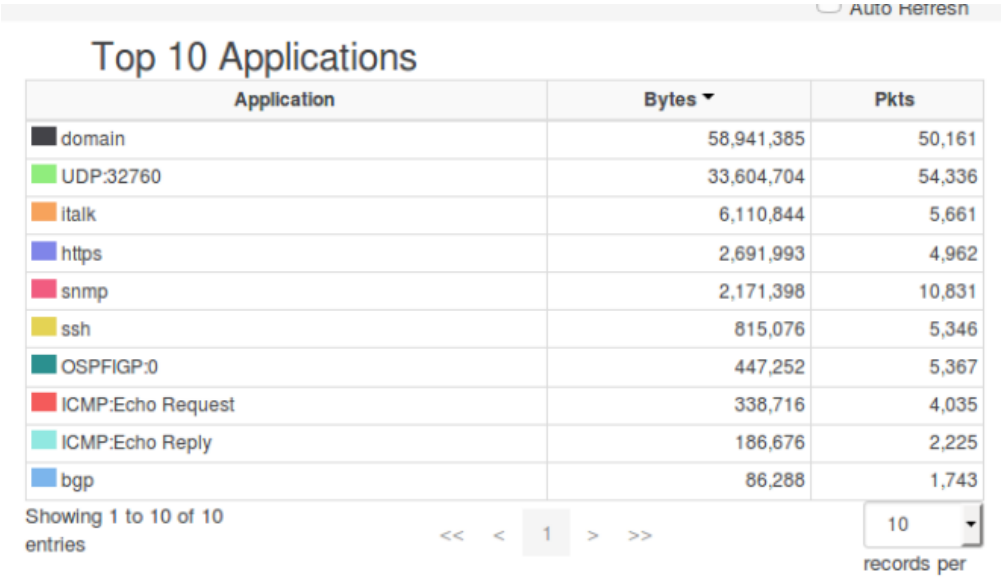


Figure 1 - Advanced Menu Window

From the advanced menu, change the summary type to "App Sources" also change the "Specific Time" section to match the time period that you feel the attack occurred. Click "Apply Selection" to confirm the changes.



Application	Bytes	Pkts
domain	58,941,385	50,161
UDP:32760	33,604,704	54,336
italk	6,110,844	5,661
https	2,691,993	4,962
snmp	2,171,398	10,831
ssh	815,076	5,346
OSPFIGP:0	447,252	5,367
ICMP:Echo Request	338,716	4,035
ICMP:Echo Reply	186,676	2,225
bgp	86,288	1,743

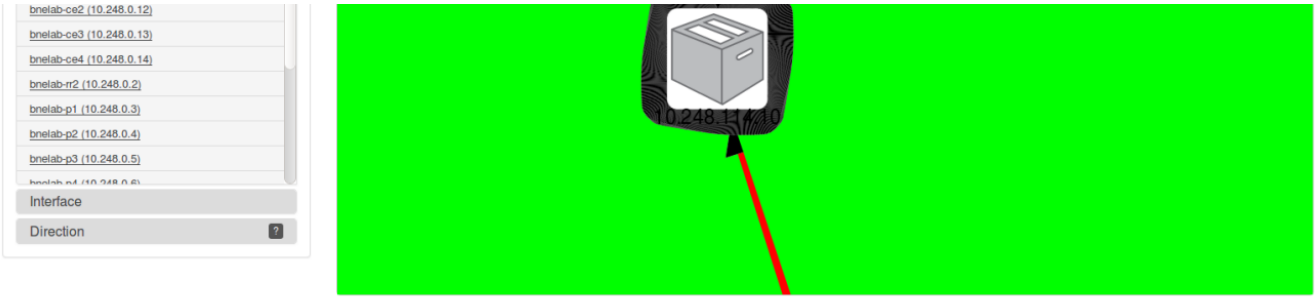
Figure 2 - Top 10 Applications

In the example in Figure 2 above we see UDP:32760 in the second row, this is displaying normal traffic for this particular network. The domain traffic in the first row seems unusual. Viewing this information we have an idea that the attack traffic is related to UDP destination port 53. In order to get a tighter vector on this traffic navigate to menu -> Views -> Conversation Map. The time interval will remain the same as the "Specific Time" filter entered in the Advanced menu earlier.

Src Port	Destination	Dst Port	TOS	Bytes	Pkts	Avg Bytes/sec	Avg P
3338	10.248.114.10	53	0	1,308	1	1	
3337	10.248.114.10	53	0	1,308	1	1	

Figure 3 - Conversation Map

The flow data table is found below the Conversation Map. Click on the time header of the flow data table to sort based on time. Next, change the records per page to 500. The conversation map will change to represent the 500 displayed flow records. Click on a flow data page that represents the time of the DDoS attack well. The conversation map above is indicating that all the traffic is focused on one destination. Disable the "Zoom Lock" on the map, then zoom into the center to determine what the attack target is.



Time	Protocol	Application	Source	Src Port	Destination	Dst Port	TOS	Bytes	Pkts	Avg Bytes/sec	Avg Pkts/s	% Bytes	% Pkts
2017-12-20T21:06:34	UDP	domain	76-205-55-26.lightspeed.cicril.sbcglobal.net	3338	10.248.114.10	53	0	1,308	1	1	0	0.0%	0.0%
2017-12-20T21:06:34	UDP	domain	227.39.33.146	3337	10.248.114.10	53	0	1,308	1	1	0	0.0%	0.0%
2017-12-20T21:06:34	UDP	domain	ANantes-652-1-224-147.w2-8.abo.wanadoo.fr	3364	10.248.114.10	53	0	1,308	1	1	0	0.0%	0.0%
2017-12-20T21:06:34	UDP	domain	224.58.205.60	3336	10.248.114.10	53	0	1,308	1	1	0	0.0%	0.0%
2017-12-20T21:06:34	UDP	domain	1.218.253.70	3371	10.248.114.10	53	0	1,308	1	1	0	0.0%	0.0%
2017-12-20T21:06:34	UDP	domain	20.151.103.254	3339	10.248.114.10	53	0	1,308	1	1	0	0.0%	0.0%

Figure 4 - Flow Data Table

As shown in Figure 4 we can see that the attack traffic is focused on the DNS server, 10.248.114.10. Looking the flow data we see all the flows are a single packet, UDP, and the destination is port 53. We can also tell that none of these are valid DNS requests because at 1,308 bytes, the packet is way too big. DNS responses can be large but a single DNS request should not be more than 150 bytes. Based on this information, an ingress policy could be written that would discard any packets larger than 150 bytes that is destined to the DNS server on UDP port 53.

In the example below you can see the process in which the opFlow server collects and analyzes NetFlow information received by the router

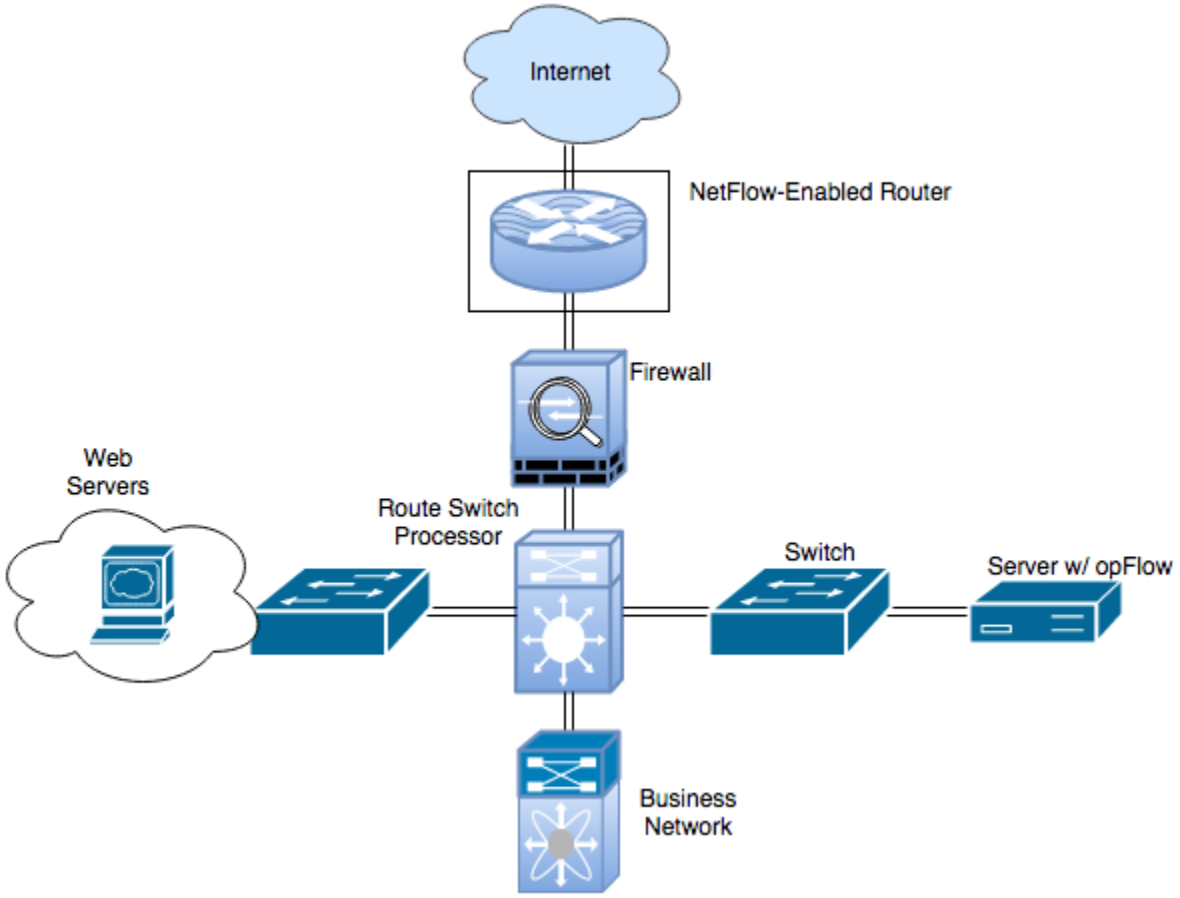


Figure 5 - NetFlow Diagram