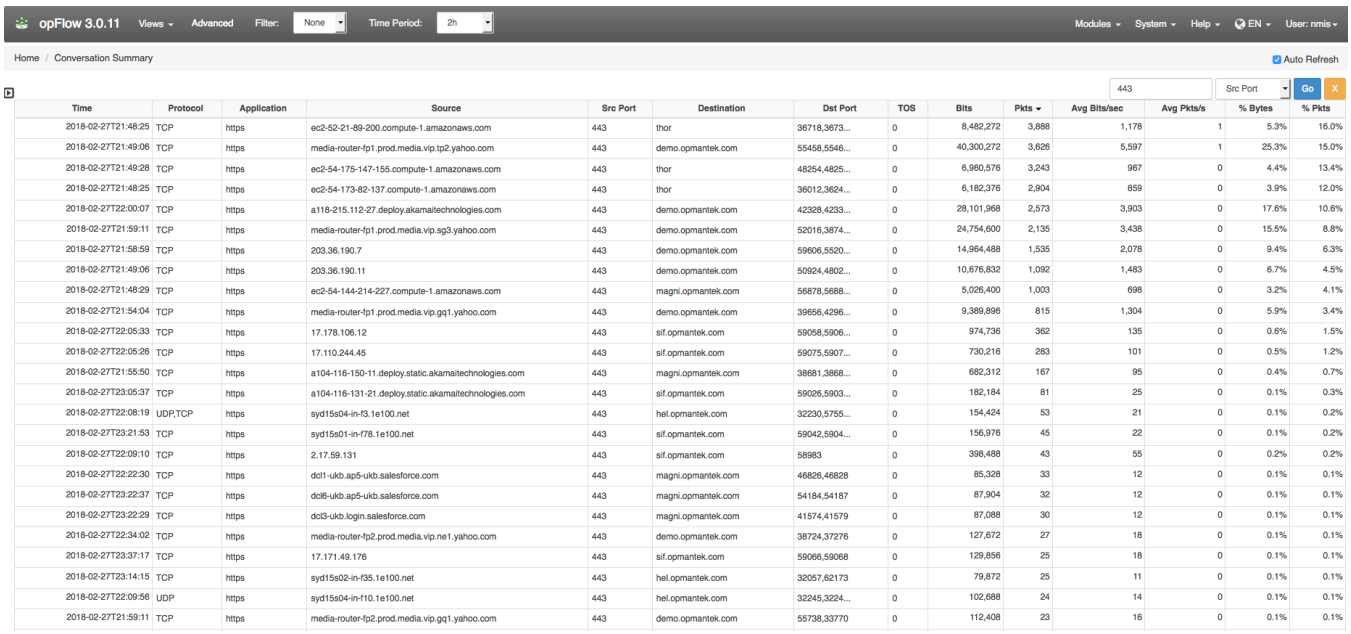
Using NetFlow/IPFIX for Anomaly Detection with opFlow

NetFlow data can be used to identify attacks on your network such as denial of service (DoS), viruses, and worms. Changes in network behavior is represented clearly with NetFlow data and understanding these deviations from normalcy can help in identifying harmful anomalies. An event or condition in the network that deviates from previously typical traffic patterns is considered an anomaly.

opFlow can detect anomalies by determining what an average network usage baseline would be and comparing it with traffic of a suspected anomaly event. DoS attacks flood the network with packets from an untrusted source and usually it is a rather large packet size. Packet sizes are normally no larger than 1500 bytes, creating an ingress policy for specific ports to discard packets larger than 1500 bytes could prevent some DoS attacks from ever occurring. opFlow clearly displays the sources and destinations of flow traffic allowing for you to see when an unknown or untrusted source is sending flow data to your network.

NetFlow collects the Packet source, Port number, Destination Packet size, and Protocol number. Understanding what ports are commonly used on your network can help you in determining if abnormal activity is coming through. Using the Conversation Summary feature in opFlow allows for a detailed look into all conversations happening on your network. There may be a lot of conversations happening across your network, in **Figure 1** below, you can see that the ports are filtered to only show Src Port 443 allowing you to see specific and relevant traffic easier. These packets can be sorted in ways that help you view and understand the information more clearly. In this example, packets received are sorted in descending order to see if the packet count is unusually higher than normal; this is why understanding what normal packet sizes are as well as the ports/sources commonly used on your network is important for any network engineer.

To view the Conversation Summary page navigate to menu -> Views -> Conversation Summary. The filter is added by simply typing the desired port in the box in the top right hand corner of the Conversation Summary page. The drop down menu to the right of the search box allows you to search for the specific Application, Source, Src Port, Destination, and Dst Port.

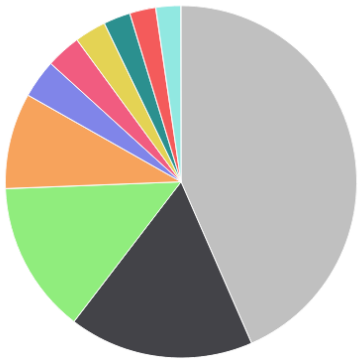


Time	Protocol	Application	Source	Src Port	Destination	Dst Port	TOS	Bits	Pkts	Avg Bits/sec	Avg Pkts/s	% Bytes	% Pkts
2018-02-27T21:48:25	TCP	https	ec2-52-21-89-200.compute-1.amazonaws.com	443	thor	36718,3673...	0	8,482,272	3,888	1,178	1	5.3%	16.0%
2018-02-27T21:49:06	TCP	https	media-router-fp1.prod.media.vip.tp2.yahoo.com	443	demo.opmantek.com	55458,5546...	0	40,300,272	3,626	5,597	1	25.3%	15.0%
2018-02-27T21:49:28	TCP	https	ec2-54-175-147-155.compute-1.amazonaws.com	443	thor	48254,4825...	0	6,960,576	3,243	967	0	4.4%	13.4%
2018-02-27T21:48:25	TCP	https	ec2-54-173-82-137.compute-1.amazonaws.com	443	thor	36012,3624...	0	6,182,376	2,904	859	0	3.9%	12.0%
2018-02-27T22:00:07	TCP	https	a118-215.112-27.deploy.akamaitechnologies.com	443	demo.opmantek.com	42328,4233...	0	28,101,968	2,573	3,903	0	17.6%	10.6%
2018-02-27T21:59:11	TCP	https	media-router-fp1.prod.media.vip.sg3.yahoo.com	443	demo.opmantek.com	52016,3874...	0	24,754,600	2,135	3,438	0	15.5%	8.8%
2018-02-27T21:58:59	TCP	https	203.36.190.7	443	demo.opmantek.com	59606,5520...	0	14,964,488	1,535	2,078	0	9.4%	6.3%
2018-02-27T21:49:06	TCP	https	203.36.190.11	443	demo.opmantek.com	50924,4802...	0	10,676,832	1,092	1,483	0	6.7%	4.5%
2018-02-27T21:48:29	TCP	https	ec2-54-144-214-227.compute-1.amazonaws.com	443	magni.opmantek.com	56878,5688...	0	5,026,400	1,003	698	0	3.2%	4.1%
2018-02-27T21:54:04	TCP	https	media-router-fp1.prod.media.vip.gq1.yahoo.com	443	demo.opmantek.com	39656,4296...	0	9,389,896	815	1,304	0	5.9%	3.4%
2018-02-27T22:05:33	TCP	https	17.178.106.12	443	sif.opmantek.com	59058,5906...	0	974,736	362	135	0	0.6%	1.5%
2018-02-27T22:05:26	TCP	https	17.110.244.45	443	sif.opmantek.com	59075,5907...	0	730,216	283	101	0	0.5%	1.2%
2018-02-27T21:55:50	TCP	https	a104-116-150-11.deploy.static.akamaitechnologies.com	443	magni.opmantek.com	38681,3868...	0	682,312	167	95	0	0.4%	0.7%
2018-02-27T23:05:37	TCP	https	a104-116-131-21.deploy.static.akamaitechnologies.com	443	sif.opmantek.com	59026,5903...	0	182,184	81	25	0	0.1%	0.3%
2018-02-27T22:08:19	UDP,TCP	https	syd15s04-in-f3.1e100.net	443	hel.opmantek.com	32230,5755...	0	154,424	53	21	0	0.1%	0.2%
2018-02-27T23:21:53	TCP	https	syd15s01-in-f78.1e100.net	443	sif.opmantek.com	59042,5904...	0	156,976	45	22	0	0.1%	0.2%
2018-02-27T22:09:10	TCP	https	2.17.59.131	443	sif.opmantek.com	58983	0	398,488	43	55	0	0.2%	0.2%
2018-02-27T22:22:30	TCP	https	dcl1-ukb.ap5-ukb.salesforce.com	443	magni.opmantek.com	46826,46828	0	85,328	33	12	0	0.1%	0.1%
2018-02-27T23:22:37	TCP	https	dcl6-ukb.ap5-ukb.salesforce.com	443	magni.opmantek.com	54184,54187	0	87,904	32	12	0	0.1%	0.1%
2018-02-27T23:22:29	TCP	https	dcl3-ukb.login.salesforce.com	443	magni.opmantek.com	41574,41579	0	87,088	30	12	0	0.1%	0.1%
2018-02-27T22:34:02	TCP	https	media-router-fp2.prod.media.vip.ne1.yahoo.com	443	demo.opmantek.com	38724,37276	0	127,672	27	18	0	0.1%	0.1%
2018-02-27T23:37:17	TCP	https	17.171.49.176	443	sif.opmantek.com	59066,59068	0	129,856	25	18	0	0.1%	0.1%
2018-02-27T23:14:15	TCP	https	syd15s02-in-f35.1e100.net	443	hel.opmantek.com	32057,62173	0	79,872	25	11	0	0.1%	0.1%
2018-02-27T22:09:56	UDP	https	syd15s04-in-f10.1e100.net	443	hel.opmantek.com	32245,3224...	0	102,688	24	14	0	0.1%	0.1%
2018-02-27T21:59:11	TCP	https	media-router-fp2.prod.media.vip.gq1.yahoo.com	443	demo.opmantek.com	55738,33770	0	112,408	23	16	0	0.1%	0.1%

Figure 1 - Conversation Summary

The default landing page for opFlow displays the Top 10 App Sources as shown in **Figure 2** below. This shows the applications that are generating the most flow data displaying their Source, Application, Bits, and Pkts. In this example, these sources are mostly coming from known servers and routers having conversations with each other. However, the application generating the most Bits is clearly Other. Other is defined by all of the other applications that are not on the Top 10 Apps list which in this case is quite a lot. The Top 10 App Sources default view can be used to detect anomalies as well. If you do not recognize a Source or Application or notice that the Other Application/Source has a larger packet count than average then this is cause to investigate. To get a clearer view of all the applications that are grouped in Other, the Conversation Summary view is recommended. If you wanted an application that is defined in the Other category to be recognized as a known application by you, you can create a Custom Application. Assigning Custom Applications to known flow data can help gain insight into your network and make it easier to notice when an anomaly is present.

Custom Application creation is detailed HERE: Creating Custom Applications



Top 10 App Sources

Source	Application	Bits	Pkts
Other	Other	516,764,552	395,504
magni.opmantek.com	UDP:32760	202,266,776	76,107
kraken.opmantek.com	UDP:32760	165,983,064	63,971
eight.opmantek.com	snmp	104,851,816	81,936
thor	snmp	41,964,744	30,962
thor	https	38,063,048	11,336
media-router-fp1.prod.media.vip.tp2.yahoo.com	https	34,437,968	3,122
demo.opmantek.com	ICMP:Echo Request	29,584,128	44,024
irukandji.opmantek.com	UDP:32760	28,615,392	21,100
a118-215.112-27.deploy.akamaitechnologies.com	https	27,382,768	2,515

Showing 1 to 10 of 10 entries « ‹ 1 › » Show 10

Figure 2 - Top 10 App Sources

More information on Anomaly Detection regarding DoS attacks can be found HERE: Detect DDoS attacks with opFlow