DAOU 다우기술

DoS Host Alert 657064

Duration: **Apr 27 21:19 - 21:31** (0:13)

DETAILS **Time:** Alert Timeframe **Units:** pps **View:** Network Boundary

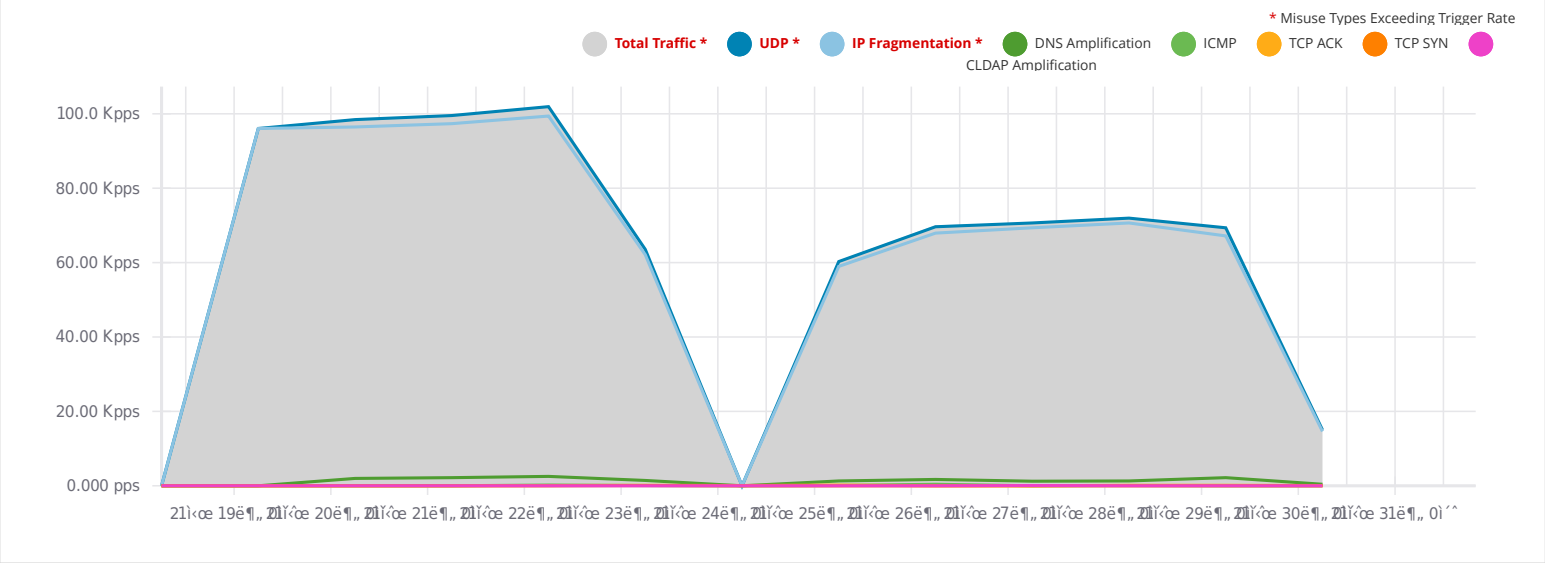
Summary

KEY INFORMATION

Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types	Managed Object	Target
High Fast Flood	993.0% of 10 Kpps	IP Fragmentation	1.1 Gbps/102.1 Kpps at Managed Object Boundary	Incoming	IP Fragmentation, Total Traffic, UDP	GigaMemory	115.71.48.31

ALERT TRAFFIC

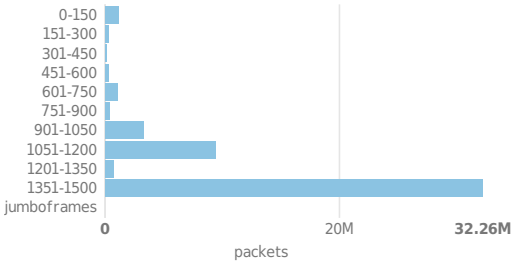
Misuse Types



Alert Characterization

Misuse Types	Total Traffic (7)	100.00%
Misuse Types	UDP (9)	99.77%
Misuse Types	IP Fragmentation (1)	97.77%
Source IP Addresses	Highly Distributed	99.98%
Destination IP Addresses	115.71.48.31/32	100.00%
Protocols	udp (17)	99.77%
Source UDP Ports	0	97.77%
Destination UDP Ports	0	97.77%
Source ASNs	NULL (0)	91.40%
Destination ASNs	NULL (0)	100.00%

Packet Size Distribution



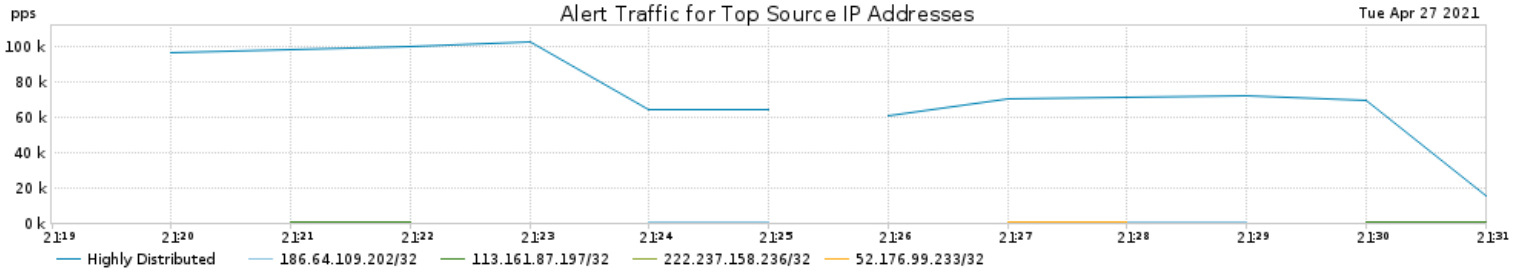
Top Traffic Patterns (last 5 min of selected timeframe)

	Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1.	Highly Distributed	UDP	--	0	115.71.48.31/32	0	MP_BS2	37.27 Kpps
2.	Highly Distributed	UDP	--	0	115.71.48.31/32	0	MP_BS1	36.18 Kpps

Traffic Details

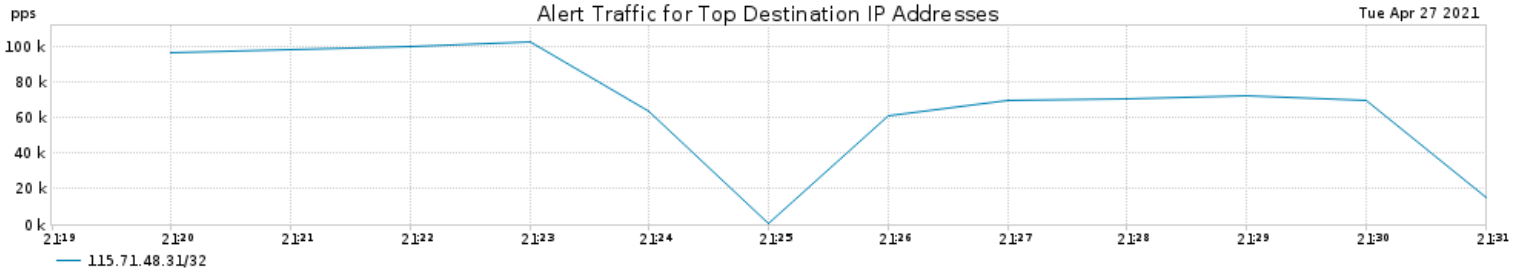
	Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1.	Highly Distributed	UDP	--	0	115.71.48.31/32	0	MP_BS2	37.27 Kpps
2.	Highly Distributed	UDP	--	0	115.71.48.31/32	0	MP_BS1	36.18 Kpps

Top 5 Items by Alert Traffic



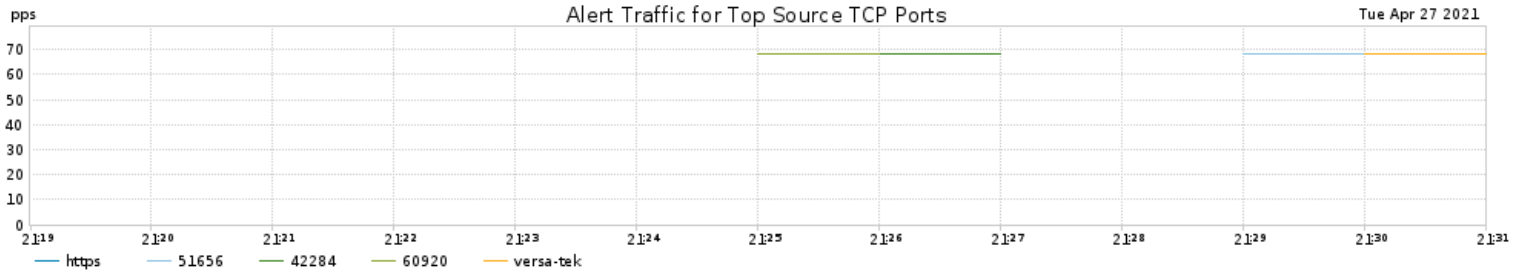
Source IP Addresses

Highly Distributed	62.94 Kpps	99.98%
186.64.109.202/32	36.00 pps	0.06%
113.161.87.197/32	36.00 pps	0.06%
222.237.158.236/32	31.00 pps	0.05%
52.176.99.233/32	31.00 pps	0.05%



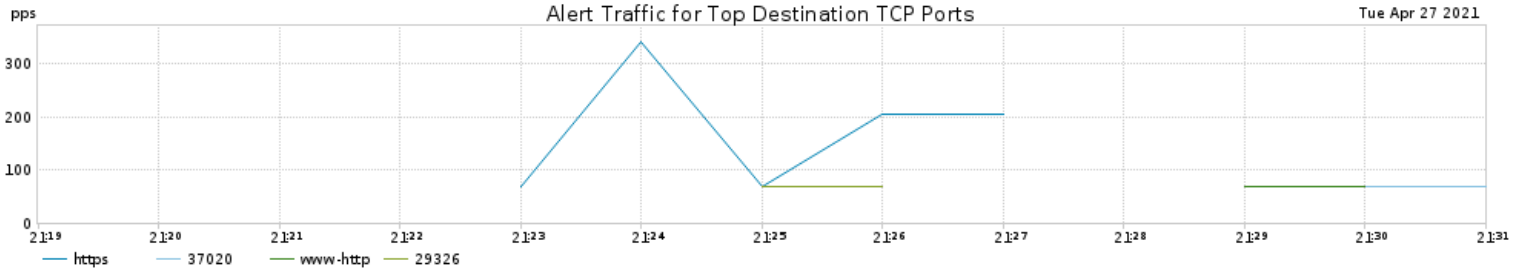
Destination IP Addresses

115.71.48.31/32	62.95 Kpps	100.00%



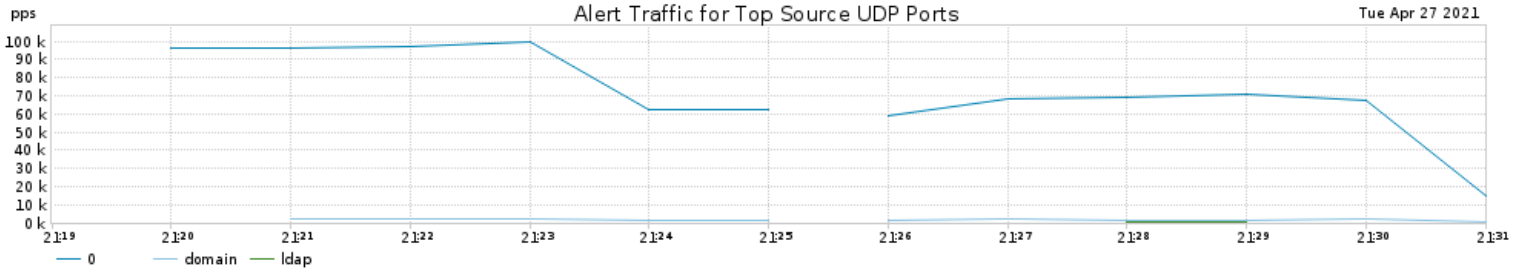
Source TCP Ports

443	https	10.00 pps	0.02%
51656		5.00 pps	0.01%
42284		5.00 pps	0.01%
60920		5.00 pps	0.01%
2610	versa-tek	5.00 pps	0.01%



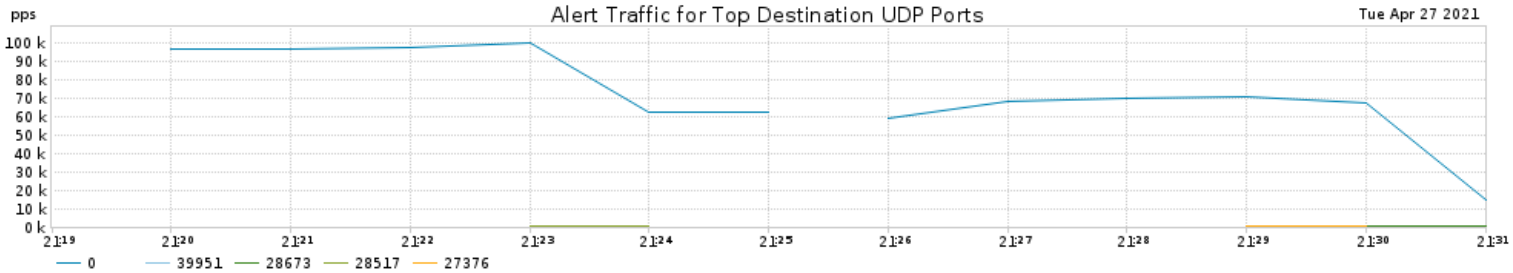
Destination TCP Ports

443	https	68.00 pps	0.11%
37020		5.00 pps	0.01%
80	www-http	5.00 pps	0.01%
29326		5.00 pps	0.01%



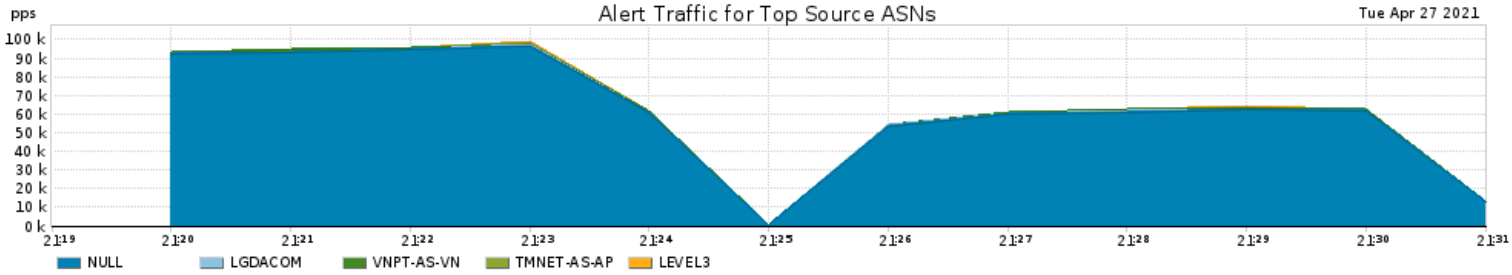
Source UDP Ports

0		61.54 Kpps	97.77%
53	domain	1.25 Kpps	1.98%
389	ldap	5.00 pps	0.01%



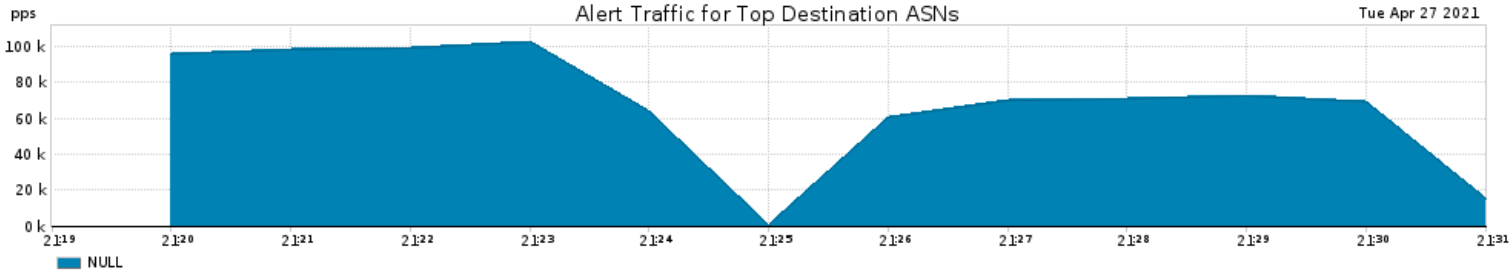
Destination UDP Ports

0		61.54 Kpps	97.77%
39951		10.00 pps	0.02%
28673		10.00 pps	0.02%
28517		10.00 pps	0.02%
27376		10.00 pps	0.02%



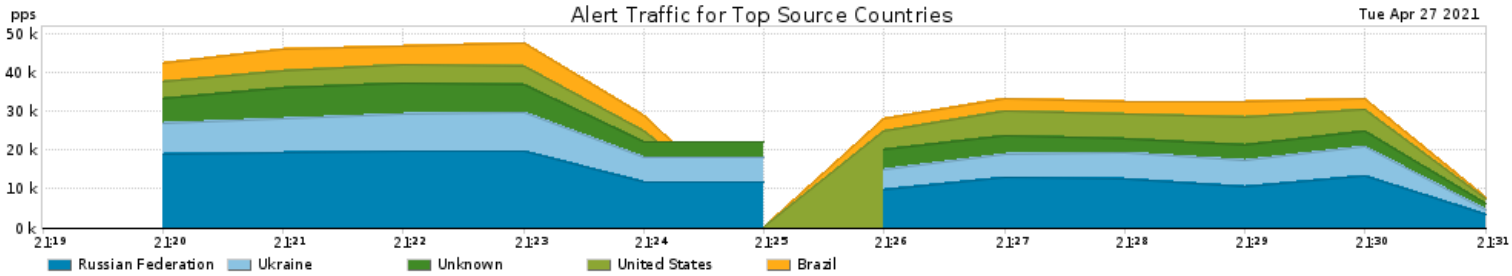
Source ASNs

0	NULL	57.53 Kpps	91.40%
3786	LGDACOM	304.00 pps	0.48%
45899	VNPT-AS-VN	299.00 pps	0.48%
4788	TMNET-AS-AP	214.00 pps	0.34%
3356	LEVEL3	136.00 pps	0.22%



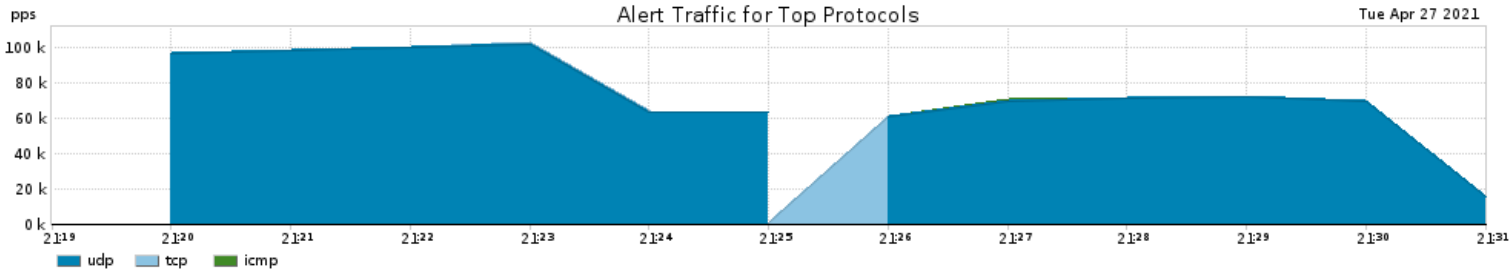
Destination ASNs

0	NULL	62.95 Kpps	100.00%



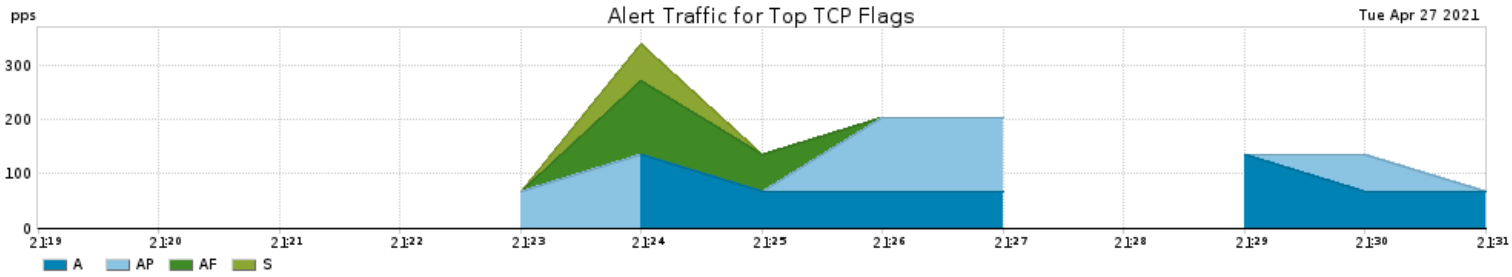
Source Countries

	Russian Federation	11.72 Kpps	18.61%
	Ukraine	5.90 Kpps	9.38%
	Unknown	4.29 Kpps	6.81%
	United States	4.10 Kpps	6.51%
	Brazil	3.17 Kpps	5.04%



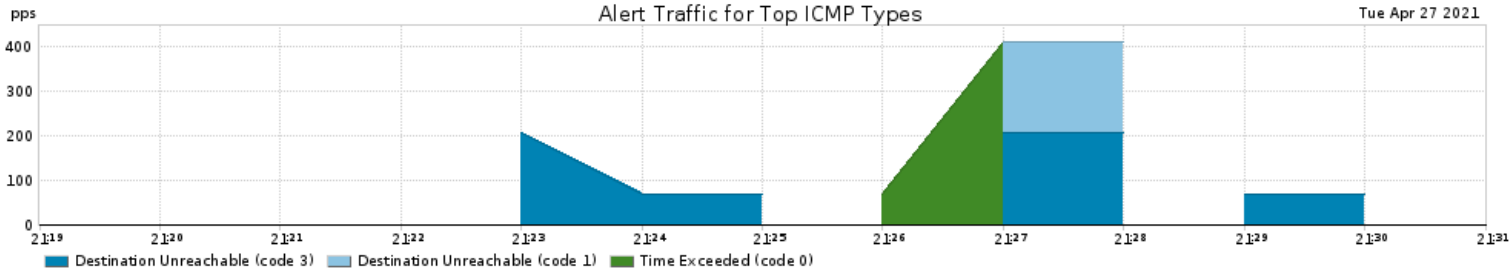
Protocols

udp	62.80 Kpps	99.77%
tcp	83.00 pps	0.13%
icmp	62.00 pps	0.10%



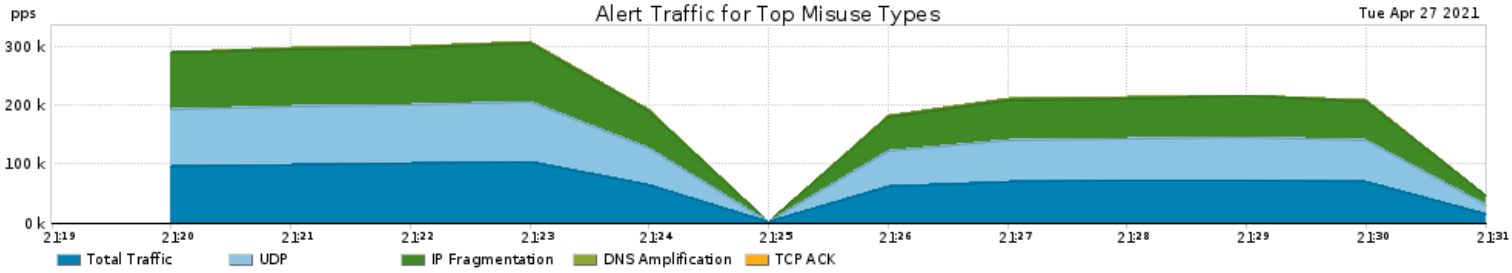
TCP Flags

A	Acknowledgement	36.00 pps	0.06%
AP	Acknowledgement, Push	26.00 pps	0.04%
AF	Acknowledgement, Finished	15.00 pps	0.02%
S	Synchronize	5.00 pps	0.01%



ICMP Types

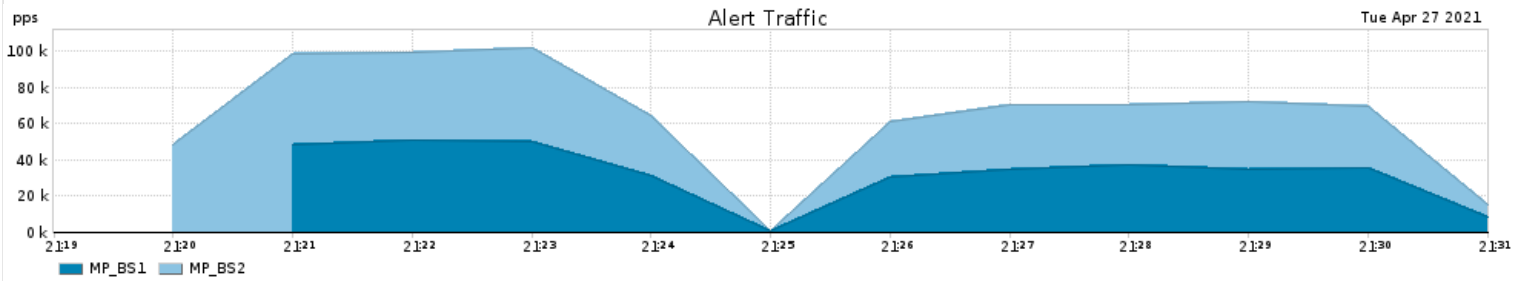
Destination Unreachable (code 3)	41.00 pps	0.07%
Destination Unreachable (code 1)	15.00 pps	0.02%
Time Exceeded (code 0)	5.00 pps	0.01%



Misuse Types

Total Traffic	62.95 Kpps	100.00%
UDP	62.80 Kpps	99.77%
IP Fragmentation	61.54 Kpps	97.77%
DNS Amplification	1.25 Kpps	1.98%
TCP ACK	62.00 pps	0.10%

Routers



Name (# Interfaces)	Severity	Interface Direction	Interface Boundary	Interface ASNs	Avg Packet Size	Max Observed	Average Observed
MP_BS1 (3)	High	-	-	-	1295	535.6 Mbps 51.1 Kpps	285.8 Mbps 27.6 Kpps
Ethernet1/1 ##SKB_1(7268058259)##		IN	Network	9318	1295	535.6 Mbps 51.1 Kpps	285.8 Mbps 27.6 Kpps
Ethernet1/50 ##MP_WS1(e 1/49)##		OUT			1294	277.6 Mbps 26.1 Kpps	141.4 Mbps 13.7 Kpps
Ethernet2/50 ##MP_WS2(e 1/49)##		OUT			1297	270.7 Mbps 25.5 Kpps	144.4 Mbps 13.9 Kpps
MP_BS2 (3)	High	-	-	-	1315	555.5 Mbps 52.6 Kpps	333.5 Mbps 31.7 Kpps
Ethernet1/1 ##SKB_2(7281067926)##		IN	Network	9318	1315	555.5 Mbps 52.6 Kpps	333.5 Mbps 31.7 Kpps
Ethernet1/50 ##MP_WS1(e 1/50)##		OUT			1317	287.3 Mbps 27.3 Kpps	172.9 Mbps 16.4 Kpps
Ethernet2/50 ##MP_WS2(e 1/50)##		OUT			1313	268.2 Mbps 25.3 Kpps	160.6 Mbps 15.3 Kpps

Annotations

Alert Classification Possible Attack

The "Total Traffic" host alert signature has been triggered at router "MP_BS1". (expected rate: 3.00 Gbps/50.00 Kpps, observed rate: 541.09 Mbps/51.58 Kpps)

auto-annotation on Tue Apr 27 21:21:45

The "UDP" host alert signature has been triggered at router "MP_BS1". (expected rate: 20.00 Kpps, observed rate: 42.50 Kpps)

auto-annotation on Tue Apr 27 21:19:45

This alert was generated due to fast flood detection. The "IP Fragmentation" host alert signature has been triggered at router "MP_BS2". (expected rate: 5.00 Kpps, observed rate: 10.04 Kpps)

auto-annotation on Tue Apr 27 21:19:05