NETSCOUT | Arbor Sightline

DoS Host Alert 124691

Duration: **Mar 17 20:00 - 20:06** (0:07)

DETAILS **Time:** Alert Timeframe **Units:** pps **View:** Router

Router (Severity): MTC-GR-01 (422%)

Summary

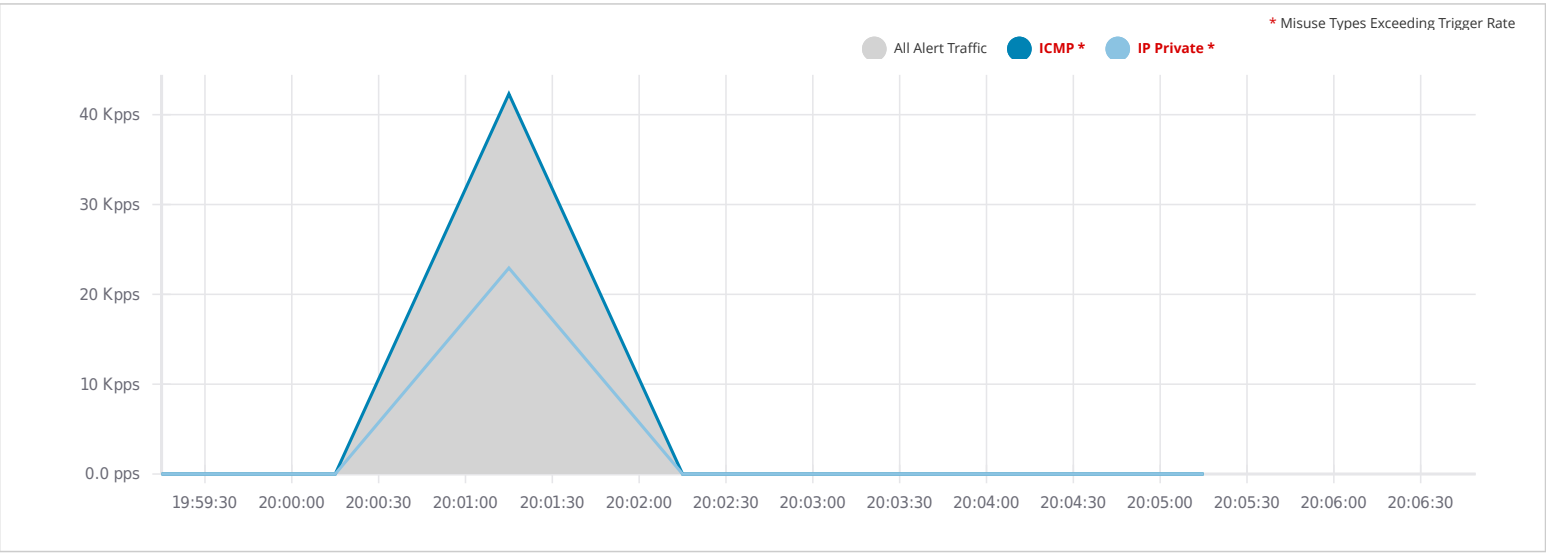
No data detected on the Network Boundary. Data shown below is for Router 'MTC-GR-01 (422%)'.

KEY INFORMATION

Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types	Managed Object	Target
High Fast Flood	422.0% of 10 Kpps	ICMP	25.3 Mbps/42.2 Kpps at MTC-GR-01	Outgoing	ICMP, IP Private	Global Detection	ff02::1

ALERT TRAFFIC

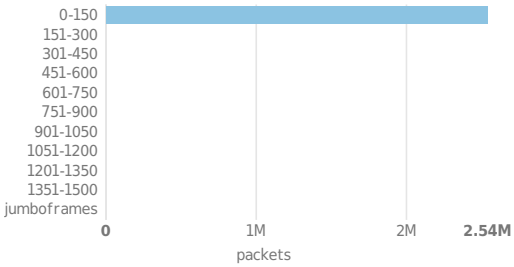
Misuse Types



Alert Characterization

Misuse Types	ICMP (0)	100.00%
Misuse Types	IP Private (3)	54.19%
Source IP Addresses	2001:504:27::d1af:0:241/128	45.81%
Source IP Addresses	fe80::8618:88ff:fea4:d301/128	44.28%
Destination IP Addresses	ff02::1/128	100.00%
Protocols	ipv6-icmp (58)	100.00%
Source Countries	Unknown	100.00%
Source ASNs	NULL (0)	100.00%
Destination ASNs	NULL (0)	100.00%
ICMP Types	IPv6 Unassigned 0 (code 136)	90.09%

Packet Size Distribution



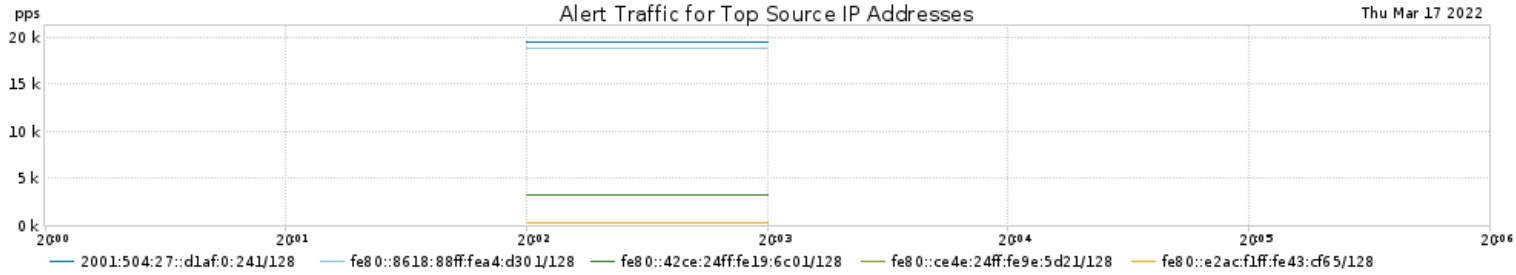
Top Traffic Patterns (last 5 min of selected timeframe)

	Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1.	2001:504:27::d1af:0:241/128	ICMPV6	--	--	ff02::1/128	--	MTC-GR-01	19.38 Kpps
2.	fe80::8618:88ff:fea4:d301/128	ICMPV6	--	--	ff02::1/128	--	MTC-GR-01	18.74 Kpps

Traffic Details

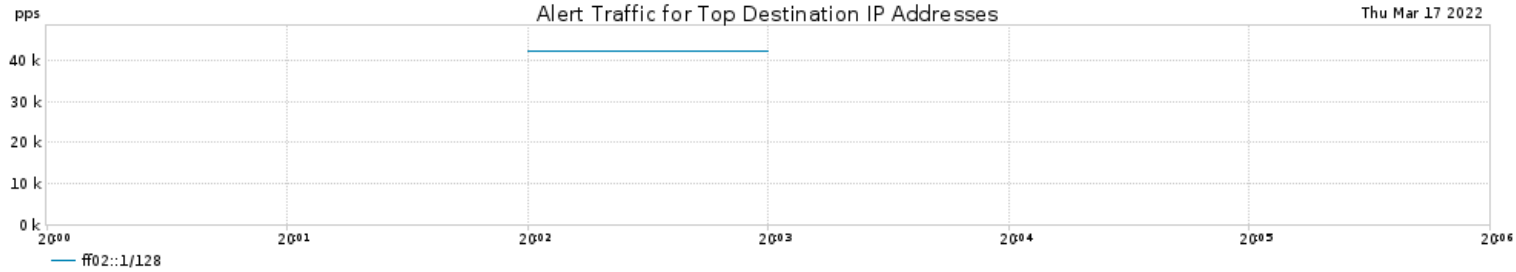
	Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1.	2001:504:27::d1af:0:241/128	ICMPV6	--	--	ff02::1/128	--	MTC-GR-01	19.38 Kpps
2.	fe80::8618:88ff:fea4:d301/128	ICMPV6	--	--	ff02::1/128	--	MTC-GR-01	18.74 Kpps

Top 5 Items by Alert Traffic



Source IP Addresses

2001:504:27::d1af:0:241/128	2.77 Kpps	45.81%
fe80::8618:88ff:fea4:d301/128	2.68 Kpps	44.28%
fe80::42ce:24ff:fe19:6c01/128	451.00 pps	7.46%
fe80::ce4e:24ff:fe9e:5d21/128	45.00 pps	0.74%
fe80::e2ac:f1ff:fe43:cf65/128	42.00 pps	0.69%



Destination IP Addresses

ff02::1/128	6.05 Kpps	100.00%

No Data

Source TCP Ports

No items available.

No Data

Destination TCP Ports

No items available.

No Data

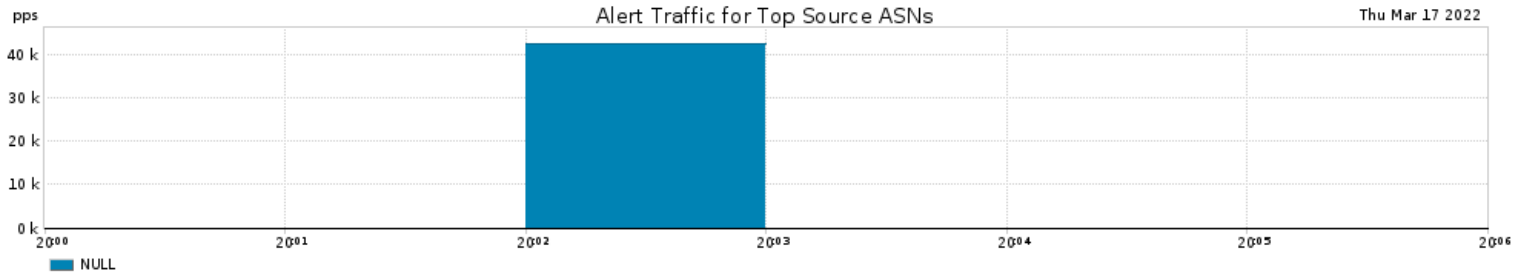
Source UDP Ports

No items available.

No Data

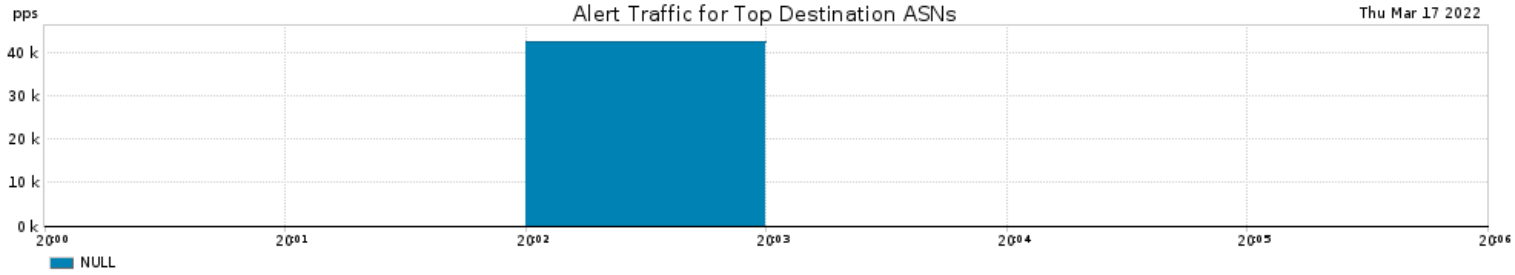
Destination UDP Ports

No items available.



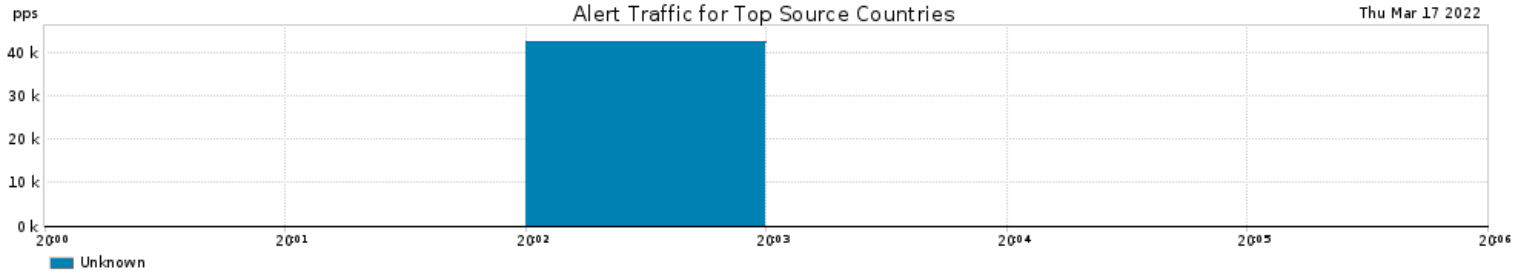
Source ASNs

0	NULL	6.05 Kpps	100.00%



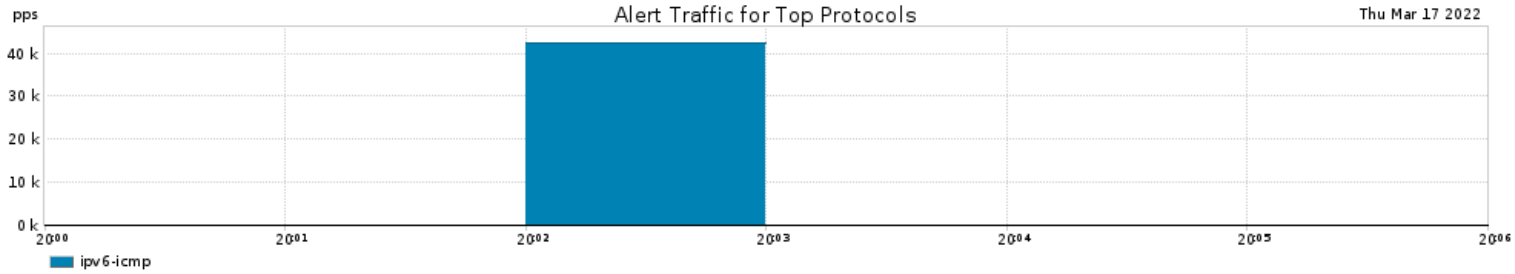
Destination ASNs

0	NULL	6.05 Kpps	100.00%



Source Countries

	Unknown	6.05 Kpps	100.00%



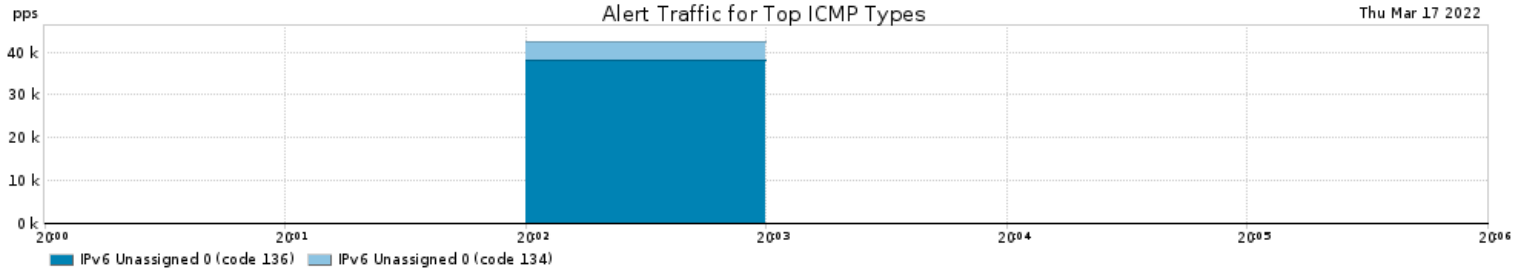
Protocols

ipv6-icmp	6.05 Kpps	100.00%

No Data

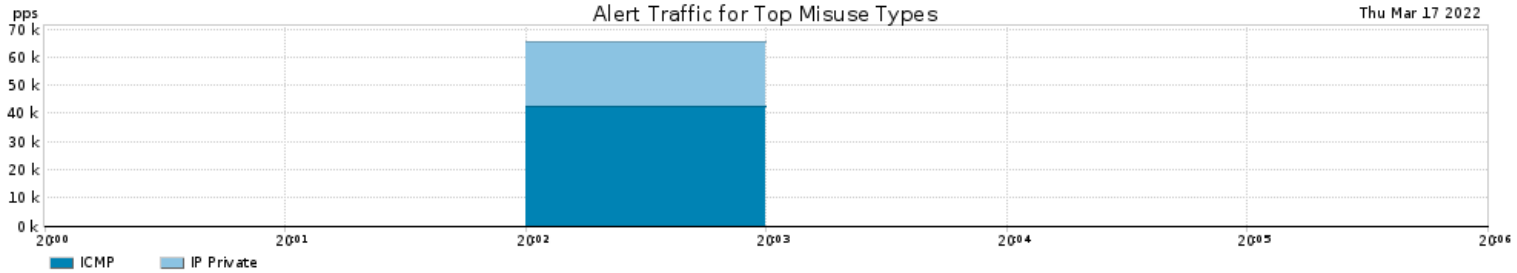
TCP Flags

No items available.



ICMP Types

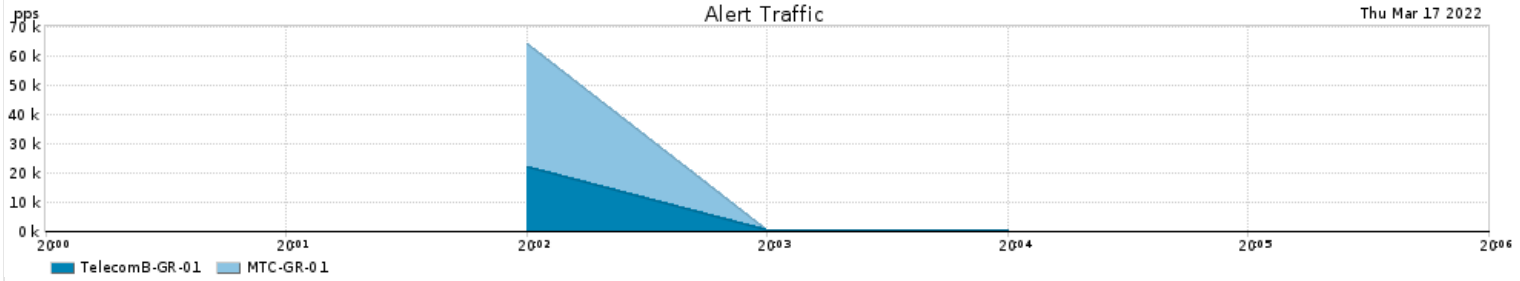
IPv6 Unassigned 0 (code 136)	5.45 Kpps	90.09%
IPv6 Unassigned 0 (code 134)	598.00 pps	9.89%



Misuse Types

ICMP	6.05 Kpps	100.00%
IP Private	3.28 Kpps	54.19%

Routers



Name (# Interfaces)	Severity	Interface Direction	Interface Boundary	Interface ASNs	Avg Packet Size	Max Observed	Average Observed
TelecomB-GR-01 (2)	**Medium**	-	-	-	77	13.8 Mbps 22.2 Kpps	2.0 Mbps 3.2 Kpps
Filtered by Router		OUT			77	13.8 Mbps 22.2 Kpps	2.0 Mbps 3.2 Kpps
HundredGigE0/9/0/3 MICE Arista port Eth6/14		IN	Network		77	13.8 Mbps 22.2 Kpps	2.0 Mbps 3.2 Kpps
MTC-GR-01 (3)	**High**	-	-	-	75	25.4 Mbps 42.3 Kpps	3.6 Mbps 6.0 Kpps
Filtered by Router		OUT			75	25.4 Mbps 42.3 Kpps	3.6 Mbps 6.0 Kpps
BVI3 Midwest Internet Cooperative Exchange (MICE)		IN	Network		75	12.7 Mbps 21.1 Kpps	1.8 Mbps 3.0 Kpps
TenGigE0/0/0/6 Loop to Te-0-2-0-6 for MICE I1 access		IN	Network		75	12.8 Mbps 21.2 Kpps	1.8 Mbps 3.0 Kpps

Annotations

Alert Classification Possible Attack

The "IP Private" host alert signature has been triggered at router "TelecomB-GR-01". (expected rate: 2.50 Kpps, observed rate: 4.07 Kpps)

auto-annotation on Thu Mar 17 20:00:45

This alert was generated due to fast flood detection. The "ICMP" host alert signature has been triggered at router "MTC-GR-01". (expected rate: 2.50 Kpps, observed rate: 11.40 Kpps)

auto-annotation on Thu Mar 17 20:00:10