

Kibana Tips

Subnet search

To filter a subnet for any variable for PA logs:

Add Filter -> Edit as Query DSL

```
{
  "query": {
    "range": {
      "<variable>": {
        "gte": "<first_subnet_ip>",
        "lt": "<last_subnet_ip>"
      }
    }
  }
}
```

Edit filter

[Edit filter values](#)

Elasticsearch Query DSL

```
1 {
2   "query": {
3     "range": {
4       "destination.address": {
5         "gte": "10.134.199.0",
6         "lt": "10.134.199.255"
7       }
8     }
9   }
10 }
```

☐ Create custom label?

Cancel

Save

source.address: 10.128.88.69 × destination.address: 10.134.199.0 to 10.134.199.255 × + Add filter

logstash-*

9 hits

Search field names

ter by type 0

destination.nat.port
destination.packets
destination.user.name
event.category
event.duration
event.start
labels
network.application
network.bytes
network.packets
network.transport
observer.hostname
observer.serial_num
panw.panos.action_flags
panw.panos.action_source

1 field sorted Full screen

	Time (@timestamp)	Document
✓	Oct 24, 2022 @ 10:47:59.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:47:59.000
✓	Oct 24, 2022 @ 10:47:42.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:47:42.000
✓	Oct 24, 2022 @ 10:47:19.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:47:19.000
✓	Oct 24, 2022 @ 10:45:44.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:45:44.000
✓	Oct 24, 2022 @ 10:45:38.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:45:38.000
✓	Oct 24, 2022 @ 10:45:35.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:45:35.000
✓	Oct 24, 2022 @ 10:45:04.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:45:04.000
✓	Oct 24, 2022 @ 10:44:58.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:44:58.000
✓	Oct 24, 2022 @ 10:44:55.000	destination.address: 10.134.199.144 source.address: 10.128.88.69 @timestamp: Oct 24, 2022 @ 10:44:55.000

Filter by Vsys:

Traffic logs are duplicated potentially so you can add the following +filter to a query to make sure you're searching the right firewall vsys!

- Datacenter Primary - panw.panos.vsys_name : SMPH-DDN (vsys14)
- Animal-Primary - panw.panos.vsys_name : SMPH-ANIMAL (vsys2)
- CSSC-Primary - panw.panos.vsys_name : SMPH-CSSC (vsys2)
- 432NM-Primary - panw.panos.vsys_name : SMPH-432NM (vsys38)